SCHAUM'S ouTlines

全美经典 学习指导系列

离散数学

〔美〕S. 利普舒尔茨　M. 利普森 著

周兴和　孙志人　张学斌 译

- 获取好成绩的最好帮手
- 涵盖了课程的所有基本内容，任一教材的补充
- 教授有效的解题技巧
- 几百道含有详细解答的习题
- 给出了最新的应用

科学出版社



麦格劳-希尔教育出版集团

全美经典学习指导系列

离 散 数 学

〔美〕S. 利普舒尔茨
M. 利普森 著

周兴和 孙志人 张学斌 译

科学出版社

麦格劳-希尔教育出版集团

2002

内 容 简 介

本书共分 15 章，包括离散数学的最基本内容. 其中包括：集合、关系、函数与算法、逻辑、向量与矩阵、计数、概率、图论、有向图、二叉树、整数的性质、代数系统、形式语言与自动机、有序集与格及布尔代数的性质. 本书的特点是叙述清楚、浅显易懂、简洁明快，内容多而不杂、占有材料量大，十分易于自学. 章后配有问题和解答与补充题，几乎占全书的一半以上的篇幅，提供了大量练习和学习的机会. 本书是一本优秀的参考书.

读者对象：大学数学及计算机等相关专业的学生.

Seymour Lipschutz, Marc Lipson: Schaum's Outline of Theory and Problems of Discrete Mathematics, Second edition

ISBN: 0-07-038045-7

图字：01－2001－1774

图书在版编目(CIP)数据

离散数学/〔美〕利普舒尔茨（Lipschutz, S.）〔美〕利普森（Lipson, M.）著；周兴和，孙志人，张学斌译. －北京：科学出版社，2002

（全美经典学习指导系列）

ISBN 7－03－009619－3

Ⅰ. 离… Ⅱ. ①利…②利…③周…④孙…⑤张… Ⅲ. 离散数学 Ⅳ. O158

中国版本图书馆 CIP 数据核字(2001)第 047879 号

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

商源印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2002 年 1 月第 一 版　　开本：A4 (890×1240)

2002 年 1 月第一次印刷　　印张：26

印数：1—5 000　　字数：747 000

定价：36.00 元

（如有印装质量问题，我社负责调换〈北燕〉）

译 者 序

本书是我们所见到的内容最为广泛的离散数学教材之一. 学生往往感到离散数学课程不仅内容多,而且繁而又难,枯燥无味. 但是本书叙述清楚,浅显易懂,简洁明快,内容多而不杂,占有材料量大而不难. 书中附有大量的例子,这些例子不仅生动活泼,语言叙述细腻,而且紧扣实际应用和日常生活,使人读来顺理成章,兴趣顿生. 对于一些有难度的重要定义和定理,这样处理之后,都不再让人感到枯燥和困难了. 问题和解答与补充题几乎占全书一半以上的篇幅. 提供了大量的习题和理解练习机会,是本书的又一大特点. 作为教材,教师可有活动范围宽广的选择空间;作为自学读本,又十分易于入门,大量获得知识,相信本书将成为我国读者学习离散数学的一本优秀参考书.

本书第一章到第五章由周兴和翻译,第六章到第十章由孙志人翻译,第十一章到第十五章由张学斌翻译,最后由周兴和负责全书的统稿和审校. 在翻译过程中,我们参阅了国内外大量的离散数学资料,力争翻译准确并保持原书的风格. 同时,对于原书中的许多(打印)错误,进行了力所能及的纠正,纠正与修改之处,恕不一一注明. 由于水平有限,不当之处在所难免,恳请读者批评指正.

最后,谨对科学出版社及其科学出版中心,特别是林鹏、吕虹、陈玉琢等的指导和帮助,以及他们为本书出版所付出的辛勤劳动致以衷心的感谢.

译者

2001 年 3 月

于南京师范大学随园

作 者 序

随着计算机科学的发展，重点研究有限系统的离散数学已经成为一门越发重要的科学.数字计算机本质上是一个有限结构，它的许多性质都可以在有限数学系统的框架下得到解释.本书包括离散数学的最基本的内容，既可作为离散数学先修课程的教材，也可作为现行课程的补充读物.

前三章讨论集合、关系、函数与算法.第四章至第七章分别讨论逻辑、向量与矩阵、计数与概率.第八章至第十章是关于图论的三章，分别讨论图、有向图和二叉树.第十一章至第十五章是相对独立的，分别讨论整数理论、代数系统、形式语言与自动机、有序集与格以及布尔代数的性质.第三章包括了对基数、可数集和计算复杂性的讨论.第八章也讨论了图的平面性、可旅行性、极小路以及 Warshall 算法和 Huffman 算法.第十三章讨论了正则表达、自动机、Turing 机以及可计算函数.基于本书内容的合理组织，改变本书章的次序不会造成学习困难也不会影响知识的连贯性.

《离散数学》第二版在内容的广度和深度上都比第一版有明显的增加.有关概率论、正则表达与正则集、二叉树、基数、计算复杂性以及 Turing 机和可计算函数等内容在第一版中或者没有出现或者仅仅是提及而已.增加这些材料的主要原因是，大部分学校都已将离散数学由一学期课程改为一学年课程.

每一章都从有关的基本定义和原理的清晰叙述开始，对于所有的定理，我们都给出了一系列的例子和其他帮助理解的材料.各章问题与解答部分的主要作用是给出增进理解学习内容的例子和该章定理的证明，而补充题则是对该章内容的完整复习.本书所包括的内容已大大超过了对初步课程要求，材料的整体组织更增进了本书作为教材的更大的灵活性，作为参考书的更强的功用性，并可以进一步提高读者学习离散数学的兴趣.

最后，我们对 McGraw-Hill Schaum 概览丛书的全体编辑人员，特别是对 Arthur Biderman 和 Maureen Walker 给予的成功合作表示衷心的感谢.

S.利普舒尔茨

M.利普森

(O-1514.0101)
责任编辑：陈玉琢

全球销量超越3000万的“全美经典学习指导系列”是您的最佳学习伴侣！

SCHAUM'S ouTlines



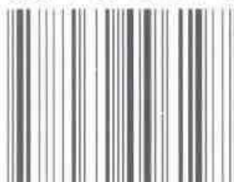
40年来最畅销的教辅系列
全美著名高校资深教授倾力之作
国内重点高校任课教师全力推荐并担当翻译
省时高效的学习辅导，全面详细的习题解答
迄今为止国内最全面的教辅系列
覆盖大学理工科专业

全美经典学习指导系列

概率和统计
统计学
离散数学
Mathematica使用指南
数理金融引论
机械振动
微分方程
统计学原理（上）
统计学原理（下）
微积分
静力学与材料力学
有限元分析
传热学
近代物理学
2000工程力学习题精解
工程力学
3000物理习题精解
流体动力学
物理学基础
材料力学
2000离散数学习题精解
工程热力学
数值分析
量子力学
有机化学习题精解
3000化学习题精解
大学化学习题精解
电路
电气工程基础
工程电磁场基础
数字信号处理
数字系统导论
数字原理
电机与机电学
基本电路分析
信号与系统
微生物学
生物化学
生物学
分子和细胞生物学
人体解剖与生理学

http://www.sciencep.com http://www.mheducation.com

ISBN 7-03-009619-3



9 787030 096197 >

McGraw Hill

ISBN 7-03-009619-3/O・1514
定 价：36.00 元

目　录

第一章　集合论

1.1 引　言

集合的概念出现于所有的数学分支中.本章引入集合论的记号和术语,这些记号和术语都是基本的,其使用将贯穿全书.

尽管要到第四章才正式讨论逻辑，但是本章引入关于表示集合的 Venn 图,并展示它在逻辑论证中的应用.到第十五章讨论布尔代数时,我们将进一步探索集合论与逻辑之间的关系.

在本章的最后,我们给出数学归纳法的正式定义.同时给出其应用实例.

1.2 集合与元素

集合可以看作是一些事物,即集合的*元素*或*成员*的全体.我们通常用大写字母表示集合,如 $A,B,X,Y,\cdots$,而用小写字母表示集合的元素,如 $a,b,x,y,\cdots$.术语"p 是 A 的元素"或等价地"p 属于 A"记作

$$p \in A.$$

而术语 p 不是 A 的元素,即 $p\in A$ 的否命题，记作

$$p \notin A.$$

在指定其元素之后,一个集合就被完全确定.这个事实的正式叙述称为外延公理.

外延公理　两个集合 A 与 B 相等当且仅当其元素相同.

如果集合 A 与 B 相等,则记 $A=B$,否则记 $A\neq B$.

集合的表示

集合有两种基本的表示方法.其一是,在可能的情况下,列出其元素.例如,

$$A = \{a,e,i,o,u\}$$

这里集合 A 的元素为字母 a,e,i,o,u.注意,元素之间用逗号隔开,并用花括号{　}将它们括起来.其二是给出集合中元素的特征性质.例如,

$$B = \{x : x \text{ 为偶数}, x > 0\}$$

读作"B 是所有大于 0 的偶数 x 的集合",注意集合 B 的元素一定是正整数.我们用一个字母,通常用 x 来表示集合的一般元素;记号中的冒号读作"使得",而后面的逗号则读作"而且".

例 1.1　(a) 上述集合 A 可以表示为

$$A = \{x : x \text{ 是英文字母}, x \text{ 是元音字母}\}.$$

显然,$b\notin A$,$e\in A$,而 $p\notin A$.

(b) 对于上述集合 B,我们不能列出其所有元素，但是通常我们将其写为

$$B = \{2,4,6,\cdots\}.$$

我们假定大家都知道其中的涵义.显然,$8\in B$,但是$-7\notin B$.

(c) 设 $E=\{x : x^2-3x+2=0\}$.换句话说,E 所含的元素恰是方程 $x^2-3x+4=0$ 的解,我们有时称之为给定方程的*解集*.因为该方程的解为 1 和 2,所以也可记 $E=\{1,2\}$.

(d) 设 $E=\{x : x^2-3x+2=0\}$,$F=\{2,1\}$而 $G=\{1,2,2,1,6/3\}$.则 $E=F=G$.显然,一个集合与其元素在集合记号中的表现形式无关.元素在集合记号中被重复书写或者改变元素在记号中的次序,都不会改变集合本身.

有些集合在本书中将经常用到，我们以特定的记号来表示它们.除非特别说明,一般设

$\mathbf{N}$=全体正整数的集合：1,2,3,…

$\mathbf{Z}$=全体整数的集合：…,−2,−1,0,1,2,…

$\mathbf{Q}$=全体有理数的集合

$\mathbf{R}$=全体实数的集合

$\mathbf{C}$=全体复数的集合

有时，尽管理论上可以列出某个集合的所有元素，但实际上却不可操作. 比如，全世界生于1976年的人的集合，尽管从理论上说，我们应该可以列出其所有元素，但我们却宁愿不这样做. 也就是说，只有当集合中所含元素很少时，我们才用列举元素的方法来表示集合，否则我们就用元素的特征性质来表示集合.

利用元素的性质表示集合的方法的正式表述为*抽象原则*.

抽象原则　给定集合 U 和性质 P，则存在集合 A 恰好包含 U 中具有性质 P 的那些元素.

1.3　全集与空集

在集合论的任何应用中，所论集合的元素往往都属于一个大的集合叫做*全集*. 例如，在平面几何中，全集由平面上的所有点构成；而在人口学研究中，全集则包含世界上所有的人. 在没有特别说明的情况下，我们将用字母 U 来表示全集.

对于给定集合 U 和性质 P，U 中满足性质 P 的元素可能不存在. 例如，集合

$$S=\{x: x\text{为正整数}, x^2=3\}$$

没有元素，因为没有正整数满足指定性质.

没有元素的集合称为*空集*或*零集*，记作∅. 空集只有一个. 即若 S,T 都是空集，则 $S=T$，因为它们恰好含有相同的元素即没有任何元素.

1.4　子　集

如果集合 A 的每个元素都是集合 B 的元素，则称 A 为 B 的一个*子集*. 此时我们也称 A *包含于* B 或 B *包含* A. 这个关系记作

$$A\subseteq B\quad\text{或}\ B\supseteq A.$$

如果 A 不是 B 的子集，即 A 至少有一个元素不属于 B，则记 $A\nsubseteq B$ 或 $B\nsupseteq A$.

例 1.2　(a) 考察集合

$$A=\{1,3,4,5,8,9\},\quad B=\{1,2,3,5,7\},\quad C=\{1,5\}.$$

则 $C\subseteq A$ 而且 $C\subseteq B$，因为 C 的元素 1,5 都是 A 和 B 的元素. 但是 $B\nsubseteq A$，因为 B 中有某些元素如 2 和 7 不属于 A. 进而，因为 A,B 和 C 的元素都必须属于全集 U，所以，全集 U 至少包含集合{1,2,3,4,5,6,7,8,9}.

(b) 设集合 $\mathbf{N},\mathbf{Z},\mathbf{Q}$ 和 $\mathbf{R}$ 的定义如 1.2. 则

$$\mathbf{N}\subseteq\mathbf{Z}\subseteq\mathbf{Q}\subseteq\mathbf{R}.$$

(c) 集合 $E=\{2,4,6\}$ 是集合 $F=\{6,2,4\}$ 的一个子集，因为属于 E 的每个元素 2,4 和 6 也都属于 F. 事实上，$E=F$. 可以证明，任何一个集合都是它自己的一个子集.

需要注意的是，集合具有下列性质.

(i) 每个集合 A 都是全集的一个子集，因为由定义，集合 A 的所有元素都属于 U. 同样地，空集∅是 A 的一个子集.

(ii) 每个集合 A 都是它自己的一个子集，因为显然 A 的元素都属于 A.

(iii) 如果 A 的每个元素都属于集合 B，而 B 的每个元素都属于集合 C，则显然 A 的每个元素都属于集合 C. 换句话说，若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$.

(iv) 如果 $A\subseteq B$ 且 $B\subseteq A$，则 A 与 B 具有相同的元素，即 $A=B$. 反之，如果 $A=B$，则因为每个集合都是它自己的子集，我们有 $A\subseteq B$ 且 $B\subseteq A$.

上述性质的正式叙述如下：

定理 1.1　(i)对任意集合 A，$\varnothing \subseteq A \subseteq U$.

(ii) 对任意集合 A，$A \subseteq A$.

(iii) 如果 $A \subseteq B$ 且 $B \subseteq C$，则 $A \subseteq C$.

(iv) $A=B$ 当且仅当 $A \subseteq B$ 且 $B \subseteq A$.

如果 $A \subseteq B$，则仍然可能有 $A=B$. 当 $A \subseteq B$ 但 $A \neq B$ 时，我们称 A 是 B 的一个真子集. 记 $A \subset B$ 表示 A 是 B 的一个真子集. 例如，假设

$$A=\{1,3\},\ B=\{1,2,3\},\ C=\{1,3,2\},$$

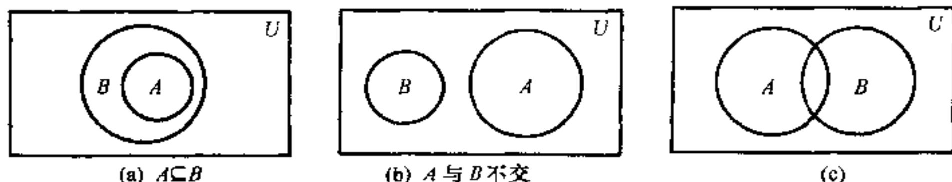
则 A 和 B 都是 C 的子集；但是 A 是 C 的一个真子集，而 B 不是 C 的真子集，因为 $B=C$.

1.5　Venn 图

Venn 图是一张表示集合的图形，在其中集合被表示为平面上的闭区域.

全集 U 由矩形表示，而其他集合则由位于矩形中的圆盘表示. 如果 $A \subseteq B$，则表示 A 的圆盘在表示 B 的圆盘内，如图 1-1(a)所示. 如果 A 与 B 不交，即它们没有公共元素，则表示 A 和 B 的两个圆盘在图中是分离的，如图 1-1(b).

然而，如果 A 与 B 是任意两个集合，则可能有某些元素在 A 中但不在 B 中；某些元素在 B 中但不在 A 中；而有些元素可能同时属于 A 与 B；有些元素可能既不在 A 中也不在 B 中. 因此，一般地，我们表示集合 A 与 B 如图 1-1(c).



(a) $A \subseteq B$　　(b) A 与 B 不交　　(c)

图 1-1

Venn 图与论证

许多论证语言本质上是关于集合的论述，从而可以用 Venn 图来表现.

因此 Venn 图有时可以用来确定一个论证是否有效. 考虑下面的例子.

例 1.3　证明下述命题为真(引自一本逻辑书，书的作者 Lewis Carroll 曾经写过《爱丽丝漫游仙境》)：

S_1：除了汤盘以外我没有一样东西是锡做的.

S_2：你给我的礼物都是很有用的.

S_3：我的汤盘都没有用.

S：你给我的礼物都不是锡做的.

(水平线以上的 S_1，S_2 和 S_3 为假设条件，水平线以下的 S 为结论. 若命题为真，则 S 为由假设 S_1，S_2 和 S_3 得到的逻辑结论.)

由 S_1，锡做的汤盘包含在汤盘的集合中，由 S_3，汤盘的集合与有用的东西的集合是不交的，因此可以画出 Venn 图，如图 1-2.

由 S_2，"你的礼物"的集合是有用的东西的集合的一个子集，因此有 Venn 图，如图 1-3.

因为"你的礼物"的集合与锡做的东西的集合不交，由上述 Venn 图，论证显然为有效.

1.6　集合的运算

本节将引入集合上的一些重要运算.

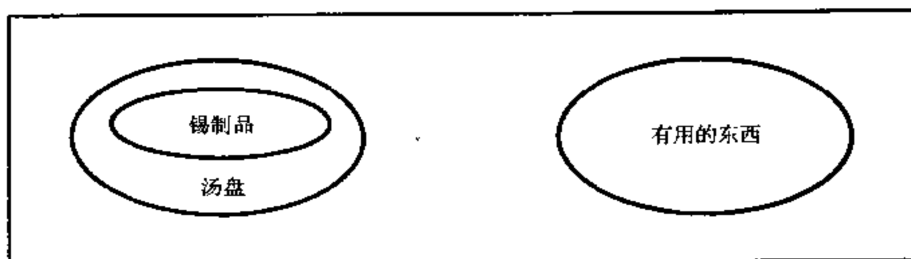


图 1-2

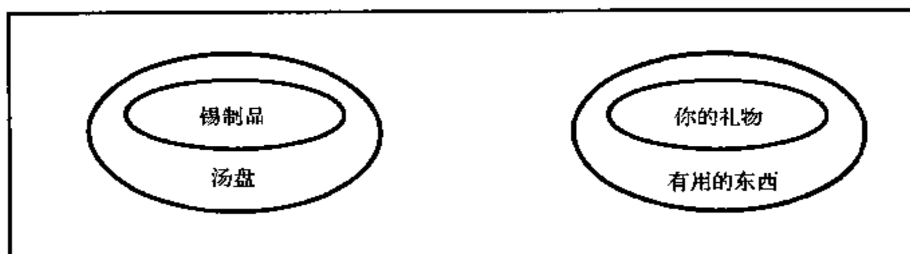


图 1-3

集合的并与交

两个集合 A 和 B 的并记作 $A\cup B$，是指属于 A 或者属于 B 的所有元素的集合，即

$$A\cup B=\{x: x\in A \text{或} x\in B\}.$$

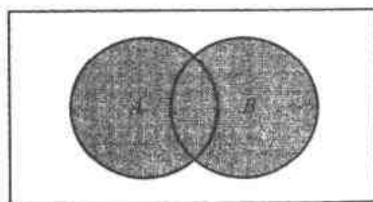
这里的"或者"即是指"与/或"意义上的或者. Venn 图 1-4(a)中的阴影部分表示 $A\cup B$.

两个集合 A 和 B 的交记作 $A\cap B$,是指同时属于 A 和 B 的所有元素的集合，

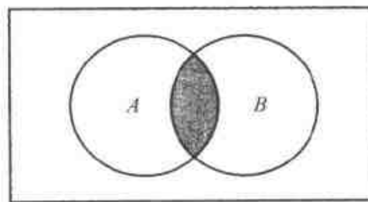
即
$$A\cap B=\{x: x\in A \text{且} x\in B\}.$$

Venn 图 1-4(b)中的阴影部分表示 $A\cap B$.

如果 $A\cap B=\varnothing$,即 A 与 B 没有公共元素，则称集合 A 与 B 是不交的.



(a) 阴影为 A ∪ B



(b) 阴影为 A ∩ B

图 1-4

例 1.4 (a) 设 $A=\{1,2,3,4\}$,$B=\{3,4,5,6,7\}$,$C=\{2,3,5,7\}$.则

$$A\cup B=\{1,2,3,4,5,6,7\},\ A\cap B=\{3,4\},$$
$$A\cup C=\{1,2,3,4,5,7\},\ A\cap C=\{2,3\}.$$

(b) 设 C 表示大学全体学生的集合,M 表示 C 中全体男生的集合,而 F 表示 C 中全体女生的集合. 因为 C 中的成员不是男生就是女生，所以

$$M\cup F=C.$$

另一方面，因为不可能有某学生既是男生又是女生，所以

$$M\cap F=\varnothing.$$

集合的包含运算与集合的并和交有着密切的关系，归纳为如下的定理.

定理 1.2 下述语句等价:$A\subseteq B$,$A\cap B=A$,$A\cup B=B$.

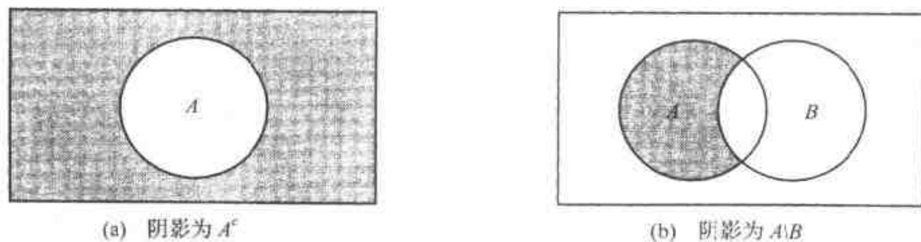
注 本定理的证明见问题 1.27，$A\subseteq B$ 的其他等价条件在问题 1.37 中给出.

集合的补

回忆前述，在某一特定场合我们所讨论的集合都是一个固定集合 U 的子集. 集合 A 的**绝对补**或者简称**补**，记作 A^c，是指所有属于 U 但不属于 A 的元素构成的集合. 即

$$A^c=\{x:x\in U,x\notin A\}.$$

有些教科书中用 A'或 $\overline{A}$ 记 A 的补. Venn 图 1-5(a)中的阴影部分表示 A^c.



(a) 阴影为 A^c　　(b) 阴影为 $A\backslash B$

图 1-5

集合 B 关于集合 A 的**相对补**或者简称为集合 A 与 B 的**差**，记作 $A\backslash B$，是由所有属于 A 但不属于 B 的元素构成的集合. 即

$$A\backslash B=\{x:x\in A,x\notin B\}.$$

集合 $A\backslash B$ 读作"A 减 B". 有许多教科书中将 $A\backslash B$ 写作 $A-B$ 或 $A\sim B$. Venn 图 1-5(b)中的阴影部分表示 $A\backslash B$.

例 1.5 设全集 $U=\mathbf{N}=\{1,2,3,\cdots\}$为全体正整数的集合. 令

$$A=\{1,2,3,4\},\quad B=\{3,4,5,6,7\}\quad C=\{6,7,8,9\}.$$

并令 $E=\{2,4,6,8,\cdots\}$为全体偶数的集合. 则

$$A^c=\{5,6,7,8,\cdots\},\ B^c=\{1,2,8,9,10,\cdots\},\ C^c=\{1,2,3,4,5,10,11,\cdots\}.$$

而

$$A\backslash B=\{1,2\},\ B\backslash C=\{3,4,5\},\ B\backslash A=\{5,6,7\},\ C\backslash E=\{7,9\}.$$

同样可得 $E^c=\{1,3,5,\cdots\}$为全体正奇数的集合.

集合的基本积

考虑 n 个不同的集合 $A_1,A_2,\cdots,A_n$. 这 n 个集合的**基本积**是一个形如

$$A_1^*\cap A_2^*\cap\cdots A_n^*$$

的集合，其中 A_i^* 或者是 A_i 或者是 A_i^c. 注意：(1) 这样的基本积共有 2^n 个；(2) 任意两个这样的基本积是不交的；(3) 全集 U 是所有这些基本积的并(问题 1.64). 下面给出这些基本积的几何描述.

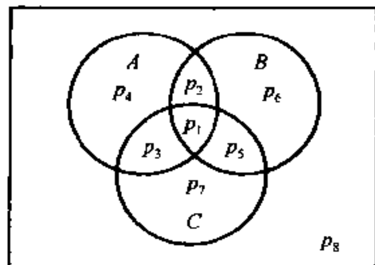
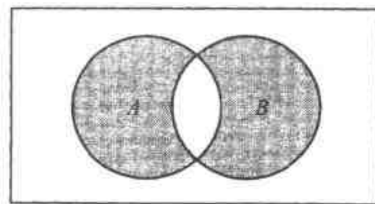


图 1-6



阴影为 $A\oplus B$

图 1-7

例 1.6 考虑三个集合 A,B,C. 列出这三个集合所构成的八个基本积如下：

$$P_1 = A \cap B \cap C,\ P_2 = A \cap B \cap C^c, P_3 = A \cap B^c \cap C,$$
$$P_4 = A \cap B^c \cap C^c,\ P_5 = A^c \cap B \cap C, P_6 = A^c \cap B \cap C^c,$$
$$P_7 = A^c \cap B^c \cap C,\ P_8 = A^c \cap B^c \cap C^c,$$

这八个基本积恰好对应着关于集合 A,B,C 的 Venn 图 1－6 中八个不交的区域.

对称差

集合 A 与 B 的*对称差*，记作 $A \oplus B$，是所有属于 A 或 B 但不同时属于 A 和 B 的元素的集合. 即

$$A \oplus B = (A \cup B) \backslash (A \cap B).$$

可以证明(问题 1.18)

$$A \oplus B = (A \backslash B) \cup (B \backslash A).$$

例如，假设 $A=\{1,2,3,4,5,6\}$ 而 $B=\{4,5,6,7,8,9\}$. 则

$$A \backslash B = \{1,2,3\},\qquad B \backslash A = \{7,8,9\},$$

从而

$$A \oplus B = \{1,2,3,7,8,9\}.$$

Venn 图 1－7 中的阴影部分表示 $A \oplus B$.

1.7 集合的代数运算和对偶性

集合的并，交和补运算满足的运算规律和等式如表 1－1 所示. 事实上，我们可以正式地叙述如下.

定理 1.3 集合满足表 1－1 所列规律.

表 1－1 集合的代数运算规律

幂等律	
(1a) $A \cup A = A$	(1b) $A \cap A = A$
结合律	
(2a) $(A \cup B) \cup C = A \cup (B \cup C)$	(2b) $(A \cap B) \cap C = A \cap (B \cap C)$
交换律	
(3a) $A \cup B = B \cup A$	(3b) $A \cap B = B \cap A$
分配律	
(4a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(4b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
同一律	
(5a) $A \cup \Phi = A$	(5b) $A \cap U = A$
(6a) $A \cup U = U$	(6b) $A \cap \Phi = \Phi$
对合律	
	(7) $(A^c)^c = A$
互补律	
(8a) $A \cup A^c = U$	(8b) $A \cap A^c = \Phi$
(9a) $U^c = \Phi$	(9b) $\Phi^c = U$
De Morgan 律	
(10a) $(A \cup B)^c = A^c \cap B^c$	(10b) $(A \cap B)^c = A^c \cup B^c$

证明有关集合运算的等式有两种方法. 一种是对于一个元素 x，去验证它同时属于方程的两边；另一种是利用 Venn 图. 例如，考虑 De Morgan 律的第一式

$$(A \cup B)^c = A^c \cap B^c.$$

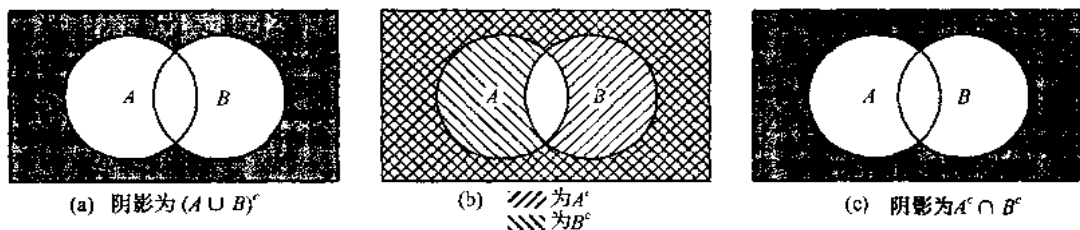
方法一 首先证明 $(A \cup B)^c \subseteq A^c \cap B^c$. 如果 $x \in (A \cup B)^c$，则 $x \notin A \cup B$. 于是，$x \notin A$ 且 $x \notin B$，因此 $x \in A^c$ 且 $x \in B^c$. 于是 $x \in A^c \cap B^c$.

然后证明 $A^c \cap B^c \subseteq (A \cup B)^c$. 设 $x \in A^c \cap B^c$. 则 $x \in A^c$ 且 $x \in B^c$，因此 $x \notin A$ 且 $x \notin B$. 于

是 $x \notin A \cup B$,从而 $x \in (A \cup B)^c$.

我们已经证明了 $(A \cup B)^c$ 的每个元素都属于 $A^c \cap B^c$,而且 $A^c \cap B^c$ 的每个元素也都属于 $(A \cup B)^c$. 这两方面的包含关系合起来就说明了等号两边的集合含有相同的元素,即 $(A \cup B)^c = A^c \cap B^c$.

方法二 由 $A \cup B$ 的 Venn 图 1－4,可以看出 $(A \cup B)^c$ 为图 1－8(a)中的阴影部分. 为求 $A^c \cap B^c$,即同时属于 A^c 和 B^c 的区域,我们用一种斜线标出 A^c,而用另一种斜线标出 B^c 如图 1－8(b). 然后,$A^c \cap B^c$ 为这两种斜线交叉的区域,如图 1－8(c). 因为标出 $(A \cup B)^c$ 和标出 $A^c \cap B^c$ 的区域完全相同,所以它们相等.



(a) 阴影为 $(A \cup B)^c$ (b) ////为 A^c \\\\\\\\为 B^c (c) 阴影为 $A^c \cap B^c$

图 1－8

对偶

注意到表 1－1 中的等式是成对出现的,如(2a),(2b)等等. 我们来考察如此成对出现的理论背景. 设 E 为集合代数运算的一个方程. 则 E 的对偶 E^* 是由将 E 中的 $\cup$, $\cap$, U 和 $\varnothing$ 依次替换为 $\cap$, $\cup$, $\varnothing$ 和 U 得到的方程. 例如

$$(U \cap A) \cup (B \cap A) = A$$

的对偶为

$$(\varnothing \cup A) \cap (B \cup A) = A.$$

在表 1－1 中成对出现的运算规律恰好是对偶的. 在集合的代数运算中,对偶原理成立,即如果一个方程 E 成立,则其对偶方程 E^* 必定成立.

1.8 有限集和计数原理

一个集合称为有限集,如果它恰含有 m 个相异的元素,其中 m 为某非负整数. 否则,称集合为无限集. 例如,空集 $\varnothing$ 和英文字母构成的集合都是有限集,而全体正偶数的集合 $\{2,4,6,\cdots\}$ 为无限集.

我们用记号 $n(A)$ 表示有限集 A 中元素的个数. 有些教科书中也用诸如 $\#(A)$, $|A|$ 或 $\text{card}(A)$ 来记 $n(A)$.

引理 1.4 如果 A, B 为不交的有限集,则 $A \cup B$ 为有限集且

$$n(A \cup B) = n(A) + n(B).$$

证明 为计算 $A \cup B$ 的元素个数,首先计算 A 中元素的个数. 因为 A 含有 $n(A)$ 个元素. 而其余只剩那些在 B 中但不在 A 中的元素. 由于 A 与 B 不交,B 中任何元素都不属于 A,因此共有 $n(B)$ 个元素在 B 中而不在 A 中. 从而 $n(A \cup B) = n(A) + n(B)$.

当 A 与 B 相交时,我们有关于 $n(A \cup B)$ 的类似公式,将在问题 1.28 中证明.

定理 1.5 若 A 与 B 均为有限集,则 $A \cup B$ 与 $A \cap B$ 均为有限集,且

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

利用这个结果,我们可以得到关于三个集合的类似公式.

推论 1.6 若 A, B 与 C 均为有限集,则 $A \cup B \cup C$ 也是有限集,且

$$\begin{aligned} n(A \cup B \cup C) = {} & n(A) + n(B) - n(C) - n(A \cap B) - n(A \cap C) \\ & - n(B \cap C) + n(A \cap B \cap C). \end{aligned}$$

我们可以利用数学归纳法(1.10)将这一结果推广到任意多个有限集的情况.

例 1.7 某学院数学系有 120 名学生,其中学习法语,德语和俄语的人数情况如下:

65 人学习法语

45 人学习德语

42 人学习俄语

20 人学习法语和德语

25 人学习法语和俄语

15 人学习德语和俄语

8 人学习所有三种语言

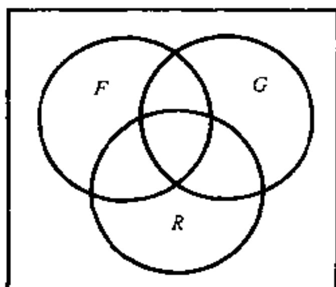


图 1-9

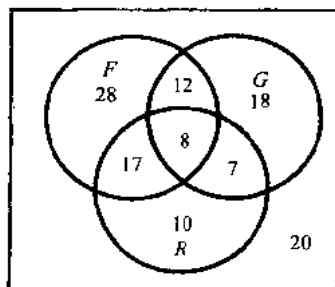


图 1-10

设 F,G 和 R 分别表示学习法语,德语和俄语的学生的集合.我们希望求出至少学习一种语言的学生人数,并且在 Venn 图 1-9 所示的八个区域中填上正确的人数.

由推论 1.6,

$$n(F\cup G\cup R)$$
$$=n(F)+n(G)+n(R)-n(F\cap G)-n(F\cap R)-n(G\cap R)+n(F\cap G\cap R)$$
$$=65+45+42-20-25-15+8=100.$$

即有 $n(F\cup G\cup R)=100$ 个学生学习至少一种语言.

现在用这个结果来填写 Venn 图中的区域.我们有:

8 个学生学习所有三种语言;

$20-8=12$ 个学生学习法语和德语但没有学习俄语;

$25-8=17$ 个学生学习法语和俄语但没有学习德语;

$15-8=7$ 个学生学习德语和俄语但没有学习法语;

$65-12-8-17=28$ 个学生仅学习法语;

$45-12-8-7=18$ 个学生仅学习德语;

$42-17-8-7=10$ 个学生仅学习俄语;

$120-100=20$ 个学生没有学习上述任一种语言.

将上述数字填入 Venn 图,结果为图 1-10.注意,其中有 $28+18-10=56$ 个学生仅学习一种语言.

1.9 集族,幂集和集合的划分

给定集合 S,有时我们需要考虑它的一些子集.这就引出了集合的集合问题.对于这种的情况,为避免混淆我们用集类或集族,表示集合的集合.如果需要考虑某给定集类中的某些集合,我们将用子类或子族称呼它们.

例 1.8 假设 $S=\{1,2,3,4\}$.用 $\mathscr{A}$ 表示 S 的恰好包含三个元素的子集族.则

$$\mathscr{A}=[\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}].$$

$\mathscr{A}$ 的元素为集合 $\{1,2,3\}$,$\{1,2,4\}$,$\{1,3,4\}$,$\{2,3,4\}$.

设 $\mathscr{B}$ 为 S 的含元素 2 和其他两个元素的子集族.则

$$\mathscr{B}=[\{1,2,3\},\{1,2,4\},\{2,3,4\}].$$

$\mathscr{B}$ 的元素为集合$\{1,2,3\}$，$\{1,2,4\}$，$\{2,3,4\}$. 因为 $\mathscr{B}$ 的每一个元素也都是 $\mathscr{A}$ 的元素，于是 $\mathscr{B}$ 是 $\mathscr{A}$ 的一个子族.（为避免混淆，有时我们用方括号记集族而不用花括号.）

幂集

对于给定的集合 S，我们可以讨论其所有子集的族. 这个族称为集合 S 的**幂集**，记作 Power(S). 如果 S 为有限集，则 Power(S)也是有限集. 事实上，Power(S)的元素个数是 2 的 $n(S)$ 方幂，即

$$n(\text{Power}(S))=2^{n(S)}.$$

（由此，S 的幂集有时也记作 2^S.）

例 1.9　设 $S=\{1,2,3\}$. 则

$$\text{Power}(S)=[\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},S].$$

注意，因为$\varnothing$是 S 的一个子集，所以空集$\varnothing$属于Power(S). 类似地，S 属于Power(S). 如上我们有，Power(S)含有 $2^3=8$ 个元素.

划分

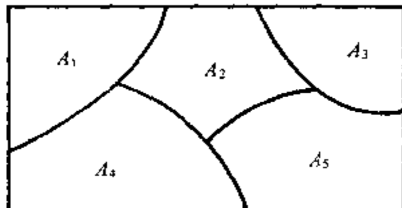


图 1-11

设 S 是一个非空集合. S 的一个**划分**是将 S 剖分为一些不交叠的非空子集. 确切地说，S 的一个划分是 S 的一族非空子集$\{A_i\}$，满足

(i) S 中每个元素 a 属于一个 A_i；

(ii) $\{A_i\}$中的集合互不相交，即若 $A_i\neq A_j$，则 $A_i\cap A_j=\varnothing$.

划分中的子集称为**胞腔**. Venn 图 1-11 表示将矩形区域内的点集划分为 A_1,A_2,A_3,A_4 和 A_5 五个胞腔.

例 1.10　考虑集合 $S=\{1,2,\cdots,8,9\}$的下列子集族：

(i) $[\{1,3,5\},\{2,6\},\{4,8,9\}]$；

(ii) $[\{1,3,5\},\{2,4,6,8\},\{5,7,9\}]$；

(iii) $[\{1,3,5\},\{2,4,6,8\},\{7,9\}]$.

则(i)不是 S 的一个划分，因为 7 不在其中的任一个子集中. (ii)也不是 S 的一个划分，因为$\{1,3,5\}$与$\{5,7,9\}$不是不交的. (iii)是 S 的一个划分.

集合运算的推广

前面，我们对两个集合定义了并和交运算. 这些运算可以被拓展到任意多个有限或无限集合.

首先考虑有限集，设 $A_1,A_2,\cdots,A_m$ 均为有限集. 这些集合的并和交分别定义为

$$A_1\cup A_2\cup\cdots\cup A_m=\bigcup_{i=1}^{m}A_i=\{x:x\in A_i,\text{对于某个 }A_i\}.$$

$$A_1\cap A_2\cap\cdots\cap A_m=\bigcap_{i=1}^{m}A_i=\{x:x\in A_i,\text{对于每个 }A_i\}.$$

即这些集合的并集是由那些至少属于其中一个集合的元素构成，而交集则由属于每个集合的元素构成.

设 $\mathscr{A}$ 为任一个集族. 集族 $\mathscr{A}$ 中集合的并和交分别定义如下：

$$\bigcup(A:A\in\mathscr{A})=\{x:x\in A,\text{对于某个 }A\in\mathscr{A}\}.$$

$$\bigcap(A:A\in\mathscr{A})=\{x:x\in A,\text{对每个 }A\in\mathscr{A}\}.$$

即并集是由那些至少属于集族 $\mathscr{A}$ 中一个集合的元素构成，而交集则由属于集族 $\mathscr{A}$ 中每个集合的元素构成.

例 1.11 考虑集合

$A_1=\{1,2,3,\cdots\}=\mathbf{N}, A_2=\{2,3,4,\cdots\}, A_3=\{3,4,5,\cdots\}, \cdots, A_n=\{n,n-1,n+2,\cdots\}$.

则这些集合的并和交分别如下：

$$\bigcup(A_n : n\in\mathbf{N})=\mathbf{N}, \quad \bigcap(A_n : n\in\mathbf{N})=\varnothing.$$

De Morgan 律对于上述拓展后的运算同样成立. 即

定理 1.7 设 $\mathscr{A}$ 为集族. 则

(i) $(\bigcup(A : A\in\mathscr{A}))^c=\bigcap(A^c : A\in\mathscr{A})$;

(ii) $(\bigcap(A : A\in\mathscr{A}))^c=\bigcup(A^c : A\in\mathscr{A})$.

1.10 数学归纳法

关于集合

$$\mathbf{N}=\{1,2,3,\cdots\}$$

的一个基本性质在证明中经常使用，即数学归纳法.

数学归纳法原理 Ⅰ 设 P 是定义于正整数集合 $\mathbf{N}$ 上的一个命题，即对 $\mathbf{N}$ 中的每个 n，$P(n)$ 或者正确或者不正确. 假设 P 具有下列两个性质：

(i) $P(1)$ 为真.

(ii) 只要 $P(n)$ 为真，$P(n+1)$ 亦为真.

则对任意正整数 P 为真.

对这个原理，我们不给出证明. 事实上，当 $\mathbf{N}$ 被公理化地引入时，这个原理一般也作为公理给出.

例 1.12 设命题 P 为：前 n 个奇数的和为 n^2，即

$$P(n): 1+3+5+\cdots+(2n-1)=n^2.$$

(注意，第 n 个奇数是 $2n-1$ 而下一个是 $2n+1$.) 当 $n=1$ 时 $P(n)$ 为真，即

$$P(1): 1=1^2.$$

假定 $P(n)$ 为真，我们在 $P(n)$ 的两边同时加上 $2n+1$，得

$$1+3+5+\cdots+(2n-1)+(2n+1)=n^2+(2n+1)=(n+1)^2$$

这就是 $P(n+1)$. 即当 $P(n)$ 为真时，$P(n+1)$ 也为真. 根据数学归纳法原理，P 对所有的 n 成立.

数学归纳法原理的另外一种形式有时是非常有用的. 尽管形式上不同，但它们却是等价的.

数学归纳法原理 Ⅱ 设 P 是定义于正整数集 $\mathbf{N}$ 上的一个命题，使得

(i) $P(1)$ 为真.

(ii) 当对于所有的 $1\leqslant k<n$，$P(k)$ 为真时，有 $P(n)$ 为真.

则 P 对于所有的正整数为真.

注 有时我们希望证明命题 P 对于整数集合

$$\{a,a+1,a+2,\cdots\}$$

为真，其中 a 为任意整数，也可能为零. 这可以通过在上述任一种归纳法中以 a 代替 1 得到.

问题与解答

集与子集

1.1 下列集合中哪些是相等的？

$$\{r,t,s\}, \quad \{s,t,r,s\}, \quad \{t,s,t,r\}, \quad \{s,r,s,t\}.$$

解 ☞ 它们全部相等. 因为元素的次序变化以及重复不改变集合本身.

1.2 设 $\mathbf{N}=\{1,2,3,\cdots\}$. 列出下列集合的元素.

(a) $A=\{x: x\in\mathbf{N}, 3<x<12\}$.

(b) $B=\{x: x\in\mathbf{N}, x$ 为偶数,且 $x<15\}$.

(c) $C=\{x: x\in\mathbf{N}, 4+x=3\}$.

解 (a) A 由 3 到 12 之间的正整数组成,因此

$$A=\{4,5,6,7,8,9,10,11\}.$$

(b) B 由小于 15 的正偶数组成,因此

$$B=\{2,4,6,8,10,12,14\}.$$

(c) 因为满足 $4+x=3$ 的正整数不存在,所以 C 没有元素. 换句话说,$C=\varnothing$.

1.3 考虑下列集合

$$\varnothing,\quad A=\{1\},\quad B=\{1,3\},\quad C=\{1,5,9\},\quad D=\{1,2,3,4,5\},$$
$$E=\{1,3,5,7,9\},\quad U=\{1,2,\cdots,8,9\}.$$

在下列每对集合之间,正确填写$\subseteq$或$\nsubseteq$符号.

(a) $\varnothing$, A; (b) A, B; (c) B, C; (d) B, E;

(e) C, D; (f) C, E; (g) D, E; (h) D, U.

解 (a) $\varnothing\subseteq A$,因为$\varnothing$是任意集合的子集.

(b) $A\subseteq B$,因为 A 的惟一元素 1 属于 B.

(c) $B\nsubseteq C$,因为 $3\in B$ 但 $3\notin C$.

(d) $B\subseteq E$,因为 B 的全部元素属于 E.

(e) $C\nsubseteq D$,因为 $9\in C$ 但 $9\notin D$.

(f) $C\subseteq E$,因为 C 的元素都属于 D.

(g) $D\nsubseteq E$,因为 $2\in D$ 但 $2\notin E$.

(h) $D\subseteq U$,因为 D 的元素都属于 U.

1.4 已知集合 $A=\{2,3,4,5\}$,$B=\{x: x\in\mathbf{N}, x$ 为偶数$\}$. 证明 A 不是 B 的一个子集.

证 只要证明 A 至少有一个元素不属于 B 即可. 显然,$3\in A$,但是由于 B 的元素必须是偶数,所以$3\notin B$. 从而 A 不是 B 的子集.

1.5 证明集合 $A=\{2,3,4,5\}$是集合 $C=\{1,2,3,\cdots,8,9\}$的一个真子集.

证 因为 A 的每一个元素都属于 C,所以 $A\subseteq C$;另一方面,$1\in C$ 但 $1\notin A$,故 $A\neq C$. 于是 A 是 C 的一个真子集.

集合的运算

在问题 1.6~1.8 中,已知集合

$$A=\{1,2,3,4,5\},\quad B=\{4,5,6,7\},\quad C=\{5,6,7,8,9\},$$
$$D=\{1,3,5,7,9\},\quad E=\{2,4,6,8\},\quad F=\{1,5,9\}.$$

并给定全集为$U=\{1,2,\cdots,9\}$.

1.6 求

(a) $A\cup B$ 和 $A\cap B$; (b) $B\cup D$ 和 $B\cap D$; (c) $A\cup C$ 和 $A\cap C$;

(d) $D\cup E$ 和 $D\cap E$; (e) $E\cup E$ 和 $E\cap E$; (f) $D\cup F$ 和 $D\cap F$.

解 回忆 $X\cup Y$ 由属于 X 或 Y(或属于两者)的元素组成,而 $X\cap Y$ 由同时属于 X 和 Y 的元素构成.

(a) $A\cup B=\{1,2,3,4,5,6,7\}$, $A\cap B=\{4,5\}$.

(b) $B\cup D=\{1,3,4,5,6,7,9\}$, $B\cap D=\{5,7\}$.

(c) $A\cup C=\{1,2,3,4,5,6,7,8,9\}=U$, $A\cap C=\{5\}$.

(d) $D\cup E=\{1,2,3,4,5,6,7,8,9\}=U$, $D\cap E=\varnothing$.

(e) $E\cup E=\{2,4,6,8\}=E$, $E\cap E=\{2,4,6,8\}=E$.

(f) $D\cup F=\{1,3,5,7,9\}=D$, $D\cap F=\{1,5,9\}=F$.

注意到 $F\subseteq D$,所以根据定理 1.2 我们有 $D\cup F=D$ 及 $D\cap F=F$.

1.7 求(a) A^c,B^c,D^c,E^c;(b) $A\setminus B,B\setminus A,D\setminus E,F\setminus D$;(c) $A\oplus B,C\oplus D,E\oplus F$.

解 回忆

(1) 补集 X^c 由在全集 U 中但不在 X 中的元素构成.

(2) 差集 $X\setminus Y$ 由属于 X 但不属于 Y 的元素构成.

(3) 对称差 $X\oplus Y$ 由属于 X 或 Y 但不同时属于两者的元素构成.

因此,

(a) $A^c=\{6,7,8,9\}$;$B^c=\{1,2,3,8,9\}$;$D^c=\{2,4,6,8\}=E$;$E^c=\{1,3,5,7,9\}=D$.

(b) $A\setminus B=\{1,2,3\}$;$B\setminus A=\{6,7\}$;$D\setminus E=\{1,3,5,7,9\}=D$;$F\setminus D=\varnothing$.

(c) $A\oplus B=\{1,2,3,6,7\}$;$C\oplus D=\{1,3,8,9\}$;$E\oplus F=\{2,4,6,8,1,5,9\}=E\cup F$.

1.8 求(a) $A\cap(B\cup E)$;(b) $(A\setminus E)^c$;(c) $(A\cap D)\setminus B$;(d) $(B\cap F)\cup(C\cap E)$.

解 (a) 首先求出 $B\cup E=\{2,4,5,6,7,8\}$. 然后 $A\cap(B\cup E)=\{2,4,5\}$.

(b) $A\setminus E=\{1,3,5\}$. 则 $(A\setminus E)^c=\{2,4,6,7,8,9\}$.

(c) $A\cap D=\{1,3,5\}$. $(A\cap D)\setminus B=\{1,3\}$.

(d) $B\cap F=\{5\}$ 而 $C\cap E=\{6,8\}$. 于是 $(B\cap F)\cup(C\cap E)=\{5,6,8\}$.

1.9 证明:不必 $B=C$ 可以有 $A\cap B=A\cap C$.

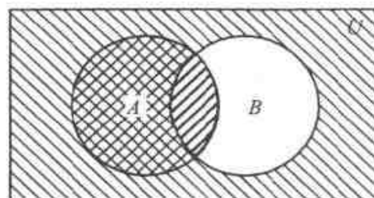
证 设 $A=\{1,2\}$,$B=\{2,3\}$ 而 $C=\{2,4\}$. 则有 $A\cap B=\{2\}$,$A\cap C=\{2\}$. 于是 $A\cap B=A\cap C$,但是 $B\neq C$.

Venn 图

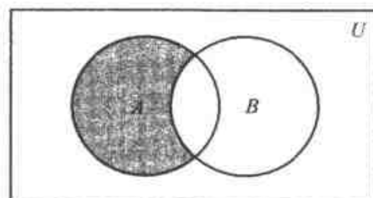
1.10 对于 Venn 图 1-1(c)中标出的任意集合 A,B,请用阴影标出下列集合:

(a) $A\cap B^c$; (b) $(B\setminus A)^c$.

解 (a) 首先用一种方向的斜线(///)标出 A. 再用另一种方向的斜线(\\\)标出 B^c(即 B 外部的区域),如图 1-12(a)所示. 两种斜线交叉部分即为交 $A\cap B^c$,如图 1-12(b)所示. 注意 $A\cap B^c=A\setminus B$. 事实上,有时将 $A\setminus B$ 定义为 $A\cap B^c$.

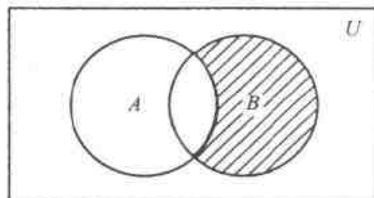


(a) 阴影为 A 与 B^c

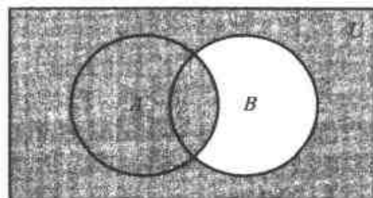


(b) 阴影为 $A\cap B^c$

图 1-12



(a) 阴影为 $B\setminus A$



(b) 阴影为 $(B\setminus A)^c$

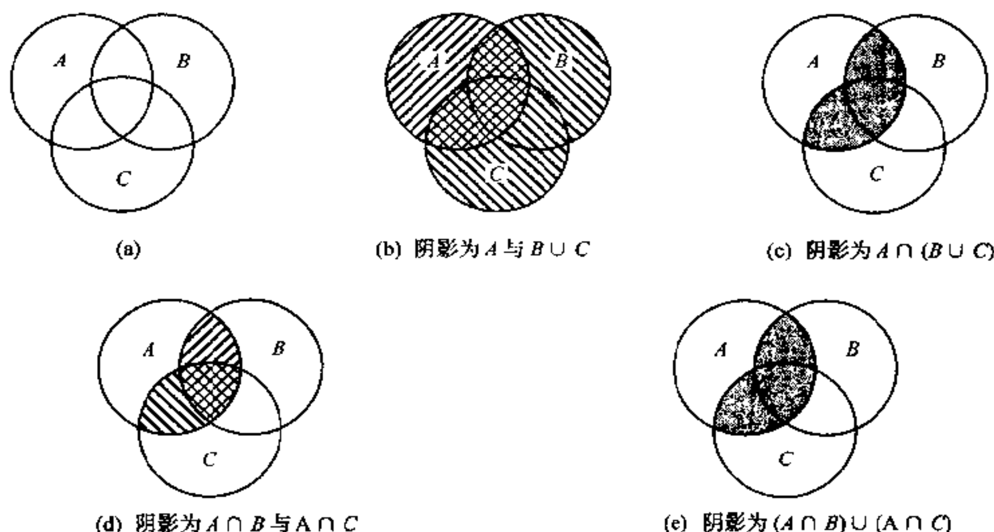
图 1-13

(b) 首先标出 $B\setminus A$(即 B 的区域但不在 A 中的部分),如图 1-13(a). 然后,这个阴影以外的部分即为 $(B\setminus A)^c$,如图 1-13(b)所示.

1.11 试用 Venn 图表示分配律 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

解 如图 1-14(a),画三个相交的圆表示 A,B,C. 然后,如图 1-14(b),将 A 用一种斜线标出,

而 $B\cup C$ 用另一种斜线标出，则两种斜线相交部分即为 $A\cap(B\cup C)$，如图 1-14(c)所示. 下一步，分别标出 $A\cap B$ 和 $A\cap C$，如图 1-14(d)，则总的被标出部分即为$(A\cap B)\cup(A\cap C)$，如图 1-14(e). 比较图 1-14(c)和 1-14(e)，即得分配律 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.



(a)　(b) 阴影为 A 与 $B\cup C$　(c) 阴影为 $A\cap(B\cup C)$

(d) 阴影为 $A\cap B$ 与 $A\cap C$　(e) 阴影为 $(A\cap B)\cup(A\cap C)$

图 1-14

1.12 确定下列命题是否为真.

S_1：我的所有朋友都是音乐家.

S_2：约翰是我的朋友.

S_3：我的邻居都不是音乐家.

S：约翰不是我的邻居.

解答 由前提 S_1 和 S_3 得到 Venn 图 1-15. 由 S_2，约翰属于与邻居集合不交的朋友集合，于是论证有效.

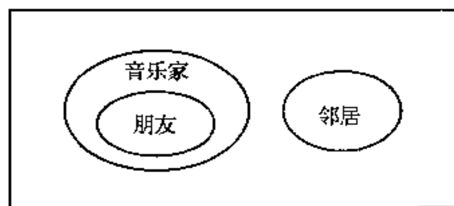


图 1-15

有限集和计数原理

1.13 判定下列集合何者为有限集.

(a) A={一年中的季节}；　(b) B={美国的州}；

(c) C={小于 1 的正整数}；　(d) D={奇数}；

(e) E={数 12 的正整数因子}；　(f) F={生活在美国的猫}.

解答 (a) 因为一年中仅有四个季节，所以 A 是有限集，$n(A)=4$.

(b) 因为美国只有 50 个州，因此 B 为有限集，$n(B)=50$.

(c) 小于 1 的正整数不存在，故 C 为空集，当然是有限集，$n(C)=0$.

(d) D是无限集.

(e) 数 12 的正整数因子为 1,2,3,4,6,12，因此 E 为有限集，$n(E)=6$.

(f) 尽管很难确定生活在美国的猫的数字，但是在一个确定的时刻，生活在美国的猫一定只有有限

只,因此 F 为有限集.

1.14 在对 60 个人进行的一项调查中,得到下列结果:

25 人阅读《新闻周刊》杂志.

26 人阅读《时代》杂志.

26 人阅读《幸运》杂志.

9 人阅读《新闻周刊》和《幸运》两种杂志.

11 人阅读《新闻周刊》和《时代》两种杂志.

8 人阅读《时代》和《幸运》两种杂志.

3 人阅读上述所有的三种杂志.

(a) 求出至少阅读一种杂志的人数.

(b) 设 N,T,F 分别表示阅读《新闻周刊》、《时代》和《幸运》杂志的人的集合,请在 Venn 图 1-16(a)中的八个区域中分别填上正确的人数.

(c) 求出只阅读一种杂志的人数.

解 (a) 我们需要求出 $n(N\cup T\cup F)$. 由推论 1.6,

$$\begin{aligned}&n(N\cup T\cup F)\\&=n(N)+n(T)+n(F)-n(N\cap T)-n(N\cap F)-n(T\cap F)+n(N\cap T\cap F)\\&=25+26+26-11-9-8+3\\&=52.\end{aligned}$$

(b) 所需 Venn 图 1-16(b)获得如下:

3 人阅读所有 3 种杂志.

$11-3=8$ 人阅读《新闻周刊》和《时代》而不是所有三种杂志.

$9-3=6$ 人阅读《新闻周刊》和《幸运》而不是所有三种杂志.

$8-3=5$ 人阅读《时代》和《幸运》而不是所有三种杂志.

$25-8-6-3=8$ 人仅阅读《新闻周刊》.

$26-8-5-3=10$ 人仅阅读《时代》.

$26-6-5-3=12$ 人仅阅读《幸运》.

$60-52=8$ 人不阅读上述任何一种杂志.

(c) $8+10+12=30$ 人仅阅读一种杂志.

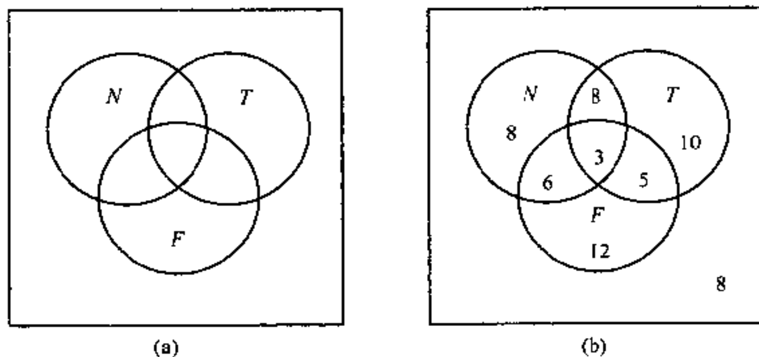


图 1-16

集合的代数运算和对偶

1.15 写出下列各方程的对偶:

(a) $(U\cap A)\cup(B\cap A)=A$;

(b) $(A\cup B\cup C)^c=(A\cup C)^c\cap(A\cup B)^c$;

(c) $(A\cap U)\cap(\varnothing\cup A^c)=\varnothing$;

(d) $(A\cap U)^c\cap A=\varnothing$.

解 在每个方程中交换$\cup$与$\cap$和U与$\varnothing$.

(a) $(\varnothing\cup A)\cap(B\cup A)=A$;

(b) $(A\cap B\cap C)^c=(A\cap C)^c\cup(A\cap B)^c$;

(c) $(A\cup\varnothing)\cup(U\cap A^c)=U$;

(d) $(A\cup\varnothing)^c\cup A=U$.

1.16 证明交换律:(a) $A\cup B=B\cup A$; (b) $A\cap B=B\cap A$.

证 (a) $A\cup B=\{x: x\in A$ 或 $x\in B\}=\{x: x\in B$ 或 $x\in A\}=B\cup A$.

(b) $A\cup B=\{x: x\in A$ 且 $x\in B\}=\{x: x\in B$ 且 $x\in A\}=B\cup A$.

1.17 证明:$(A\cup B)\cap(A\cup B^c)=A$.

证

论述	理由
1. $(A\cup B)\cap(A\cup B^c)=A\cup(B\cap B^c)$	分配律
2. $B\cap B^c=\varnothing$	互补律
3. $(A\cup B)\cap(A\cup B^c)=A\cup\varnothing$	代换
4. $A\cup\varnothing=A$	恒等律
5. $(A\cup B)\cap(A\cup B^c)=A$.	代换

1.18 证明:$(A\cup B)\backslash(A\cap B)=(A\backslash B)\cup(B\backslash A)$.(于是,这两者都可以用来定义$A\oplus B$.)

证 利用$X\backslash Y=X\cap Y^c$和表1-1中的定律及De Morgan律,可得

$$\begin{aligned}&(A\cup B)\backslash(A\cap B)\\&=(A\cup B)\cap(A\cap B)^c\\&=(A\cup B)\cap(A^c\cup B^c)\\&=(A\cap A^c)\cup(A\cap B^c)\cup(B\cap A^c)\cup(B\cap B^c)\\&=\varnothing\cup(A\cap B^c)\cup(B\cap A^c)\cup\varnothing\\&=(A\cap B^c)\cup(B\cap A^c)\\&=(A\backslash B)\cup(B\backslash A).\end{aligned}$$

集类

1.19 写出集合$A=[\{1,2,3\},\{4,5\},\{6,7,8\}]$的元素.

解 A是一个集类,其元素为集合$\{1,2,3\},\{4,5\},\{6,7,8\}$.

1.20 考虑问题1.19中的集类A,判断下列命题是否正确.

(a) $1\in A$; (b) $\{1,2,3\}\subseteq A$; (c) $\{6,7,8\}\in A$; (d) $\{\{4,5\}\}\subseteq A$; (e) $\varnothing\in A$;
(f) $\varnothing\subseteq A$.

解 (a) 错误.因为1不是A的一个元素.

(b) 错误.因为$\{1,2,3\}$是A的一个元素,而不是A的一个子集.

(c) 正确.因为$\{6,7,8\}$是A的一个元素.

(d) 正确.因为$\{\{4,5\}\}$是一个以$\{4,5\}$作为元素的集合,是A的一个子集.

(e) 错误.空集不是A的一个元素,已知集合A中所列出的三个元素并没有空集.

(f) 正确.空集是任意集合的子集,当然也是一个集类的子集.

1.21 确定集合$A=\{a,b,c,d\}$的幂集Power(A).

解 因为Power(A)的元素为A的子集,所以

$$\begin{aligned}\text{Power}(A)=[&A,\{a,b,c\},\{a,b,d\},\{a,c,d\},\{b,c,d\},\{a,b\},\{a,c\},\\&\{a,d\},\{b,c\},\{b,d\},\{c,d\},\{a\},\{b\},\{c\},\{d\},\varnothing]\end{aligned}$$

由此所知,Power(A)具有$2^4=16$个元素.

1.22 设$S=\{$红,蓝,绿,黄$\}$.试判断下述何者为S的划分.

(a) $P_1=[\{$红$\},\{$蓝,绿$\}]$. (b) $P_2=[\{$红,蓝,绿,黄$\}]$.

(c) $P_3=[\varnothing,\{$红,蓝$\},\{$绿,黄$\}]$. (d) $P_4=[\{$蓝$\},\{$红,黄,绿$\}]$.

解☞ (a) 不是. 因为黄不属于任一胞腔.

(b) 是. 因为 P_2 是 S 的一个仅含惟一元素 S 的划分.

(c) 不是. 因为空集 $\varnothing$ 不能属于一个划分.

(d) 是. 因为 S 的每个元素恰出现于一个胞腔中.

1.23 求 $S=\{1,2,3\}$ 的一个划分.

解☞ 注意到 S 的划分只能包含 1,2 或 3 个胞腔. 对应于这些胞腔数的划分如下:

(1): $[S]$.

(2): $[\{1\},\{2,3\}]$, $[\{2\},\{1,3\}]$, $[\{3\},\{1,2\}]$.

(3): $[\{1\},\{2\},\{3\}]$.

杂题

1.24 证明命题 P:前 n 个正整数之和为 $\frac{1}{2}n(n+1)$. 即

$$P(n):\quad 1+2+3+\cdots+n=\frac{1}{2}n(n+1).$$

证☞ 因为

$$P(1):\ 1=\frac{1}{2}(1)(1+1).$$

所以,当 $n=1$ 时,命题成立.

假定 $P(n)$ 成立,我们在 $P(n)$ 的两端分别加上 $n+1$,得

$$\begin{aligned}&1+2+3+\cdots+n+(n+1)\\&=\frac{1}{2}n(n+1)+(n+1)\\&=\frac{1}{2}[n(n+1)+2(n+1)]\\&=\frac{1}{2}[(n+1)(n+2)],\end{aligned}$$

这就是 $P(n+1)$. 即当 $P(n)$ 为真时, $P(n+1)$ 也为真. 根据归纳原理, P 对所有正整数 n 成立.

1.25 对于 $n\geqslant 0$,证明下列命题成立.

$$P(n):\quad 1+2+2^2+2^3+\cdots+2^n=2^{n+1}-1.$$

证☞ 因为 $1=2^1-1$,所以 $P(0)$ 成立.

假定 $P(n)$ 成立,我们在 $P(n)$ 的两端同时加上 2^{n+1},得

$$\begin{aligned}&1+2+2^2+\cdots+2^n+2^{n+1}\\&=2^{n+1}-1+2^{n+1}\\&=2(2^{n+1})-1\\&=2^{n+2}-1,\end{aligned}$$

这就是 $P(n+1)$. 即当 $P(n)$ 为真时, $P(n+1)$ 也为真. 根据归纳原理, P 对所有 $n\geqslant 0$ 成立.

1.26 证明: $(A\cap B)\subseteq A\subseteq(A\cup B)$ 和 $(A\cap B)\subseteq B\subseteq(A\cup B)$.

证☞ 因为 $A\cap B$ 的每个元素都同时属于 A 和 B,所以有若 $x\in(A\cap B)$,则 $x\in A$, 即 $(A\cap B)\subseteq A$. 进而,若 $x\in A$,则 $x\in(A\cup B)$(由 $A\cup B$ 的定义),所以 $A\subseteq(A\cup B)$. 综上得到 $(A\cap B)\subseteq A\subseteq(A\cup B)$. 同理可证 $(A\cap B)\subseteq B\subseteq(A\cup B)$.

1.27 证明定理 1.2: 下列是等价的: $A\subseteq B$, $A\cap B=A$ 以及 $A\cup B=B$.

证☞ 假设 $A\subseteq B$ 并且 $x\in A$. 则 $x\in B$,因此 $x\in A\cap B$ 且 $A\subseteq A\cap B$. 据问题1.26, $(A\cap B)\subseteq A$. 从而 $A\cap B=A$. 另一方面,假设 $A\cap B=A$ 且设 $x\in A$. 则 $x\in(A\cap B)$,因此 $x\in A$ 且 $x\in B$. 从而 $A\subseteq B$. 上述两个方面的结果说明 $A\subseteq B$ 与 $A\cap B=A$ 等价.

再假设 $A\subseteq B$. 设 $x\in(A\cup B)$. 则 $x\in A$ 或 $x\in B$. 如果 $x\in A$,则因 $A\subseteq B$ 有 $x\in B$. 在两种情况下均有 $x\in B$. 因此 $A\cup B\subseteq B$. 由问题 1.26, $B\subseteq A\cup B$. 从而 $A\cup B=B$. 现在假设 $A\cup B=B$ 且设 $x\in A$. 则由集合并的定义有 $x\in A\cup B$. 因此 $x\in B=A\cup B$. 从而 $A\subseteq B$. 综合上述有 $A\subseteq B$ 等价于 $A\cup B=B$.

于是，$A\subseteq B$，$A\cap B=A$ 以及 $A\cup B=B$ 是等价的.

1.28 证明定理 1.5：若 A 与 B 均为有限集，则 $A\cup B$ 与 $A\cap B$ 都是有限集，且

$$n(A\cup B)=n(A)+n(B)-n(A\cap B).$$

证 若 A 与 B 都是有限集，则显然 $A\cup B$ 与 $A\cap B$ 均为有限集.

假如我们首先求 A 的元素个数，再求 B 的元素个数，则所有在 $A\cap B$ 中的元素都被计算了两次. 因此，

$$n(A\cup B)=n(A)+n(B)-n(A\cap B).$$

另法(问题 1.36)，A 为 $A\setminus B$ 与 $A\cap B$ 的不交并，B 为 $B\setminus A$ 与 $A\cap B$ 的不交并，$A\cup B$ 为 $A\setminus B$，$A\cap B$ 和 $B\setminus A$ 的不交并. 根据引理 1.4，

$$\begin{aligned}n(A\cup B)&=n(A\setminus B)+n(A\cap B)+n(B\setminus A)\\&=n(A\setminus B)+n(A\cap B)+n(B\setminus A)+n(A\cap B)-n(A\cap B)\\&=n(A)+n(B)-n(A\cap B).\end{aligned}$$

补 充 题

集和子集

1.29 下列集合中，哪些是相等的?

$A=\{x: x^2-4x+3=0\}$； $B=\{x: x^2-3x+2=0\}$； $C=\{x: x\in\mathbf{N}, x<3\}$；

$D=\{x: x\in\mathbf{N}, x$ 为奇数$, x<5\}$； $E=\{1,2\}$； $F=\{1,2,1\}$； $G=\{3,1\}$； $H=\{1,1,3\}$.

1.30 设全集为 $U=\{a,b,c,\cdots,y,z\}$. 列举下列集合的元素. 进而，如果存在，找出其中相等的集合.

$A=\{x: x$ 为元音字母$\}$； $B=\{x: x$ 为单词 little 中的字母$\}$；

$C=\{x: x$ 在字母 f 的前面$\}$； $D=\{x: x$ 为单词 title 中的字母$\}$.

1.31 设 $A=\{1,2,\cdots,8,9\}$，$B=\{2,4,6,8\}$，$C=\{1,3,5,7,9\}$，$D=\{3,4,5\}$，$E=\{3,5\}$. 在下述条件下，上述集合中何者可以等于集合 X?

(a) X 与 B 不交. (b) $X\subseteq D$ 但 $X\not\subseteq B$.

(c) $X\subseteq A$ 但 $X\not\subseteq C$. (d) $X\subseteq C$ 但 $X\not\subseteq A$.

集合的运算

在问题 1.32～1.34 中，设 $U=\{1,2,3,\cdots,8,9\}$，$A=\{1,2,5,6\}$，$B=\{2,5,7\}$，$C=\{1,3,5,7,9\}$.

1.32 求(a) $A\cap B$ 与 $A\cap C$；(b) $A\cup B$ 与 $B\cup C$；(c) A^c 与 C^c.

1.33 求(a) $A\setminus B$ 与 $A\setminus C$； (b) $A\oplus B$ 与 $A\oplus C$.

1.34 求(a) $(A\cup C)\setminus B$；(b) $(A\cup B)^c$；(c) $(B\oplus C)\setminus A$.

1.35 设 $A=\{a,b,c,d,e\}$，$B=\{a,b,d,f,g\}$，$C=\{b,c,e,y,h\}$，$D=\{d,e,f,g,h\}$. 求

(a) $A\cup B$； (b) $B\cap C$； (c) $C\setminus D$； (d) $A\cap(B\cup D)$；

(e) $B\setminus(C\cup D)$； (f) $(A\cap D)\cup B$； (g) $(A\cup D)\setminus C$； (h) $B\cap C\cap D$；

(i) $(C\setminus A)\setminus D$； (j) $A\oplus B$； (k) $A\oplus C$； (l) $(A\oplus D)\setminus B$.

1.36 设 A,B 为任意集合. 证明：

(a) A 是 $A\setminus B$ 与 $A\cap B$ 的不交并.

(b) $A\cup B$ 是 $A\setminus B$，$A\cap B$ 及 $B\setminus A$ 的不交并.

1.37 证明下列命题：

(a) $A\subseteq B$ 当且仅当 $A\cap B^c=\varnothing$.

(b) $A\subseteq B$ 当且仅当 $A^c\cup B=U$.

(c) $A\subseteq B$ 当且仅当 $B^c\subseteq A^c$.

(d) $A\subseteq B$ 当且仅当 $A\setminus B=\varnothing$.

(与定理 1.2 的结果相比较)

1.38 证明吸收律：(a) $A\cup(A\cap B)=A$；(b) $A\cap(A\cup B)=A$.

1.39 公式 $A\setminus B=A\cap B^c$ 利用交和补运算定义了集合的差运算. 试求一个公式利用交和补定义集合的并运算.

Venn 图

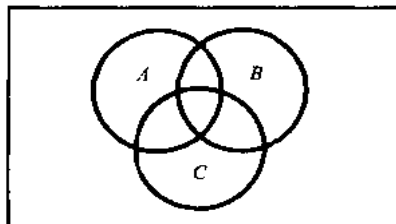


图 1-17

1.40 对于 Venn 图 1-17 所示的集合 A,B,C,标出下列集合:
(a) $A\setminus(B\cup C)$; (b) $A^c\cap(B\cup C)$; (c) $A^c\cap(C\setminus B)$.

1.41 利用 Venn 图 1-6 和例 1.6,将下列每个集合写为基本积的不交并.
(a) $A\cap(B\cup C)$. (b) $A^c\cap(B\cup C)$. (c) $A\cup(B\setminus C)$.

1.42 画出 Venn 图表示集合 A,B,C. 其中 $A\subseteq B$,集合 B 与 C 不交,但是 A 与 C 有公共元素.

集合的代数运算和对偶

1.43 写出下列方程的对偶.
(a) $A\cup B=(B^c\cap A^c)^c$. (b) $A=(B^c\cap A)\cup(A\cap B)$.
(c) $A\cup(A\cap B)=A$. (d) $(A\cap B)\cup(A^c\cap B)\cup(A\cap B^c)\cup(A^c\cap B^c)=U$.

1.44 利用表 1-1 中的定律证明下列等式.
(a) $(A\cap B)\cup(A\cap B^c)=A$.
(b) $A\cup(A\cap B)=A$.
(c) $A\cup B=(A\cap B^c)\cup(A^c\cap B)\cup(A\cap B)$.

有限集和计数原理

1.45 判定下列集合中何者为有限集.
(a) 平行于 x 轴的直线的集合.
(b) 全体英文字母的集合.
(c) 能被数 5 整除的数的集合.
(d) 地球上的动物的集合.
(e) 方程

$$x^{27}+26x^{18}-17x^{11}+7x^3-10=0$$

的解的集合.
(f) 过原点(0,0)的圆的集合.

1.46 利用定理 1.5 证明推论 1.6:若 A,B,C 为有限集,则 $A\cup B\cup C$ 也是有限集,且
$n(A\cup B\cup C)=n(A)+n(B)+n(C)-n(A\cap B)-n(A\cap C)-n(B\cap C)+n(A\cap B\cap C)$.

1.47 为了调查消费者对于汽车中的(A)空调,(R)收音机,(P)电动窗等三种流行可选件的需求倾向,人们对一个地方销售商售出的 25 辆新汽车进行了一次调查,结果如下:
15 辆车装有空调.
12 辆车装有收音机.
11 辆车装有电动窗.
5 辆同时装有空调和电动窗.
9 辆同时装有空调和收音机.
4 辆同时装有收音机和电动窗.
3 辆同时选择了上述三种配件.
求下列数据:(a) 仅有电动窗;(b) 仅有空调;(c) 仅有收音机;(d) 具有收音机和电动窗但没有空调;(e) 具有空调和收音机但没有电动窗;(f) 仅选择一种配件;(g) 没有选择上述任何一种配件.

集类

1.48 求 $A=\{1,2,3,4,5\}$ 的幂集 Power(A).

1.49 给定 $A=[\{a,b\},\{c\},\{d,e,f\}]$.
(a) 判定下述正确与否:
(i) $a\in A$, (ii) $\{c\}\subseteq A$, (iii) $\{d,e,f\}\in A$, (iv) $\{\{a,b\}\}\subseteq A$, (v) $\varnothing\subseteq A$.
(b) 求 A 的幂集.

1.50 设 A 为有限集，且 $n(A)=m$. 证明 Power(A)具有 2^m 个元素.

划分

1.51 设 $X=\{1,2,\cdots,8,9\}$. 判定下列子集族是否为 X 的一个划分.

(a) $[\{1,3,6\},\{2,8\},\{5,7,9\}]$.

(b) $[\{1,5,7\},\{2,4,8,9\},\{3,5,6\}]$.

(c) $[\{2,4,5,8\},\{1,9\},\{3,6,7\}]$.

(d) $[\{1,2,7\},\{3,5\},\{4,6,8,9\},\{3,5\}]$.

1.52 设 $S=\{1,2,3,4,5,6\}$. 判定下列子集族是否为 S 的一个划分.

(a) $P_1=[\{1,2,3\},\{1,4,5,6\}]$. (b) $P_2=[\{1,2\},\{3,5,6\}]$.

(c) $P_3=[\{1,3,5\},\{2,4\},\{6\}]$. (d) $P_4=[\{1,3,5\},\{2,4,6,7\}]$.

1.53 判定下列子集族是否为正整数集 $\mathbf{N}$ 的一个划分.

(a) $[\{n: n>5\},\{n: n<5\}]$.

(b) $[\{n: n>5\},\{0\},\{1,2,3,4,5\}]$.

(c) $[\{n: n^2>11\},\{n: n^2<11\}]$.

1.54 设$[A_1,A_2,\cdots,A_m]$和$[B_1,B_2,\cdots,B_n]$都是某集合 X 的划分. 证明集族

$$P=[A_i\cap B_j: i=1,\cdots,m,j=1,\cdots,n]\backslash\varnothing$$

也是 X 的一个划分(称为交叉划分). (注意我们删除了空集$\varnothing$.)

1.55 设 $X=\{1,2,\cdots,8,9\}$. 对于 X 的下述给定划分，求出其交叉划分.

$$P_1=[\{1,3,5,7,9\},\{2,4,6,8\}],\quad P_2=[\{1,2,3,4\},\{5,7\},\{6,8,9\}].$$

Venn 图与论证

1.56 求一个 Venn 图说明下列论证正确.

S_1:婴儿是不讲理的.

S_2:没有人瞧不起能管理鳄鱼的人.

S_3:不讲理的人被人瞧不起.

S:婴儿不能管理鳄鱼.

(本例引自 Lewis Carroll 著《符号逻辑》，他也是《爱丽丝漫游仙境》的作者)

1.57 给定下列假设条件：

S_1：所有字典都是有用的.

S_2：玛莉只有传奇小说.

S_3：传奇小说都没有用处.

试确定下列结论是否成立：(a) 传奇小说不是字典. (b) 玛莉没有字典. (c) 所有有用的书都是字典.

归纳法

1.58 证明：$2+4+6+\cdots+2n=n(n+1)$.

1.59 证明：$1+4+7+\cdots+(3n-2)=2n(3n-1)$.

1.60 证明：$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\frac{1}{5\cdot 7}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{1}{2n+1}$.

1.61 证明：$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$.

杂题

1.62 设 $\mathbf{N}=\{1,2,3,\cdots\}$为全集，并且 $A=\{x: x\leqslant 6\}$，$B=\{x: 4\leqslant x\leqslant 9\}$，$C=\{1,3,5,7,9\}$，$D=\{2,3,5,7,8\}$. 求：(a) $A\oplus B$；(b) $B\oplus C$；(c) $A\cap(B\oplus D)$；(d) $(A\cap B)\oplus(A\cap D)$.

1.63 证明对称差的性质：

(i) $A\oplus(B\oplus C)=(A\oplus B)\oplus C$ (结合律).

(ii) $A\oplus B=B\oplus A$ (交换律).

(iii) 若 $A\oplus B=A\oplus C$,则 $B=C$ (消去律).

(iv) $A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$ (分配律).

1.64 在一个全集 U 中考虑 n 个不同的集合 $A_1,A_2,\cdots,A_n$. 证明:

(a) n 个集合存在 2^n 个基本积.

(b) 任意两个基本积为不交的.

(c) U 为所有基本积的并.

补充题答案

1.29 $B=C=E=F$; $A=D=G=H$.

1.30 $A=\{a,e,i,o,u\}$; $B=D=\{l,i,t,e\}$; $C=\{a,b,c,d,e\}$.

1.31 (a) C 与 E; (b) D 与 E; (c) A,B,D; (d) 无.

1.32 (a) $A\cap B=\{2,5\}$; $A\cap C=\{1,5\}$. (b) $A\cup B=\{1,2,5,6,7\}$; $B\cup C=\{1,2,3,5,7,9\}$. (c) $A^c=\{3,4,7,8,9\}$; $C^c=\{2,4,6,8\}$.

1.33 (a) $A\setminus B=\{1,6\}$; $A\setminus C=\{2,6\}$. (b) $A\oplus B=\{1,6,7\}$; $A\oplus C=\{2,3,6,7,9\}$.

1.34 (a) $(A\cup C)\setminus B=\{1,3,6,9\}$. (b) $(A\cup B)^c=\{3,4,8,9\}$. (c) $(B\oplus C)\setminus A=\{3,9\}$.

1.35 (a) {a,b,c,d,e,f,g}; (b) {b,g}; (c) {b,c}; (d) {a,b,d,e}; (e) {a}; (f) {a,b,d,e,f,g}; (g) {a,d,f}; (h) {g}; (i) $\varnothing$; (j) {c,e,f,g}; (k) {a,d,y,h}; (l) {c,h}.

1.39 $A\cup B=(A^c\cap B^c)^c$.

1.40 见图 1-18.

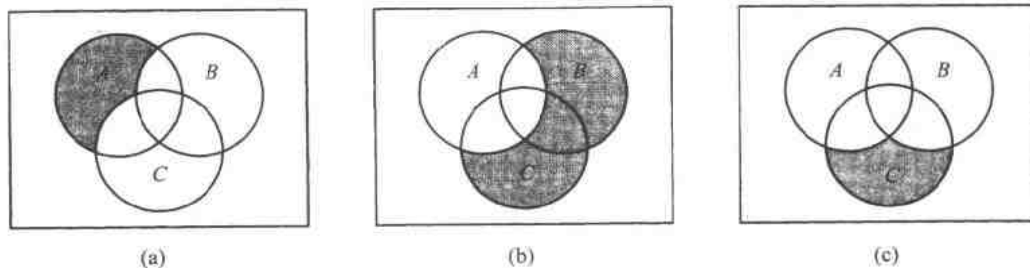


图 1-18

1.41 (a) $(A\cap B\cap C)\cup(A\cap B\cap C^c)\cup(A\cap B^c\cap C)$.

(b) $(A^c\cap B\cap C^c)\cup(A^c\cap B\cap C)\cup(A^c\cap B^c\cap C)$.

(c) $(A\cap B\cap C)\cup(A\cap B\cap C^c)\cup(A\cap B^c\cap C)\cup(A^c\cap B\cap C^c)\cup(A\cap B^c\cap C^c)$.

1.42 不存在这样的 Venn 图. 如果 A 与 C 有一个公共元素,设为 x,且 $A\subseteq B$,则 x 也必须属于 B. 于是 B 和 C 也必须具有一个公共元素.

1.43 (a) $A\cap B=(B^c\cup A^c)^c$; (b) $A=(B^c\cup A)\cap(A\cup B)$; (c) $A\cap(A\cup B)=A$; (d) $(A\cup B)\cap(A^c\cup B)\cap(A\cup B^c)\cap(A^c\cup B^c)=\varnothing$.

1.45 (a) 无限; (b) 有限; (c) 无限; (d) 有限; (e) 有限; (f) 无限.

1.47 如图 1-19,首先将 Venn 图中的 A(空调),R(收音机),W(电动窗)填上已知数据. 然后,(a) 5; (b) 4; (c) 2; (d) 4; (e) 6; (f) 11; (g) 23; (h) 2.

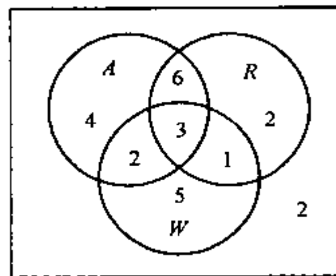


图 1-19

1.48 Power(A)具有 $2^5=32$ 个元素如下:

[$\varnothing$,{1},{2},{3},{4},{5},{1,2},{1,3},{1,4},{1,5},{2,3},{2,4},{2,5},{3,4},{3,5},{4,5},{1,2,3},{1,2,4},{1,2,5},{2,3,4},{2,3,5},{3,4,5},{1,3,4},{1,3,5},{1,4,5},{2,4,5},{1,2,3,4},{1,2,3,5},{1,2,4,5},{1,3,4,5},{2,3,4,5},A].

1.49 (a) (i) 错; (ii) 错; (iii) 对; (iv) 对; (v) 对. (b) 注意到 $n(A)=3$,所以 Power(A)具有 $2^3=8$ 个元素.

Power$(A)=\{A,[\{a,b\},\{c\}],[\{a,b\},\{d,e,f\}],[\{c\},\{d,e,f\}],[\{a,b\}],[\{c\}],[\{d,e,f\}],\varnothing\}$

1.50 设 x 为 Power(A)中的任意一个元素. 对于每个 $a\in A$,存在两种可能性:$a\in A$ 或 $a\notin A$. 但是 A 中具有 m 个元素,因此共有 $2\times2\times\cdots\times2=2^m$ 个不同的集合 X. 即 Power(A)具有 2^m 个元素.

1.51 (a) 否, (b) 否, (c) 是, (d) 是.

1.52 (a) 否, (b) 否, (c) 是, (d) 否.

1.53 (a) 否, (b) 否, (c) 是.

1.55 $P=[\{1,3\},\{5,7\},\{9\},\{2,4\},\{8\}]$.

1.56 由三个前提得到 Venn 图,如图 1-20. 婴儿的集合与能管理鳄鱼的人的集合是不交的. 换言之,结论 S 成立.

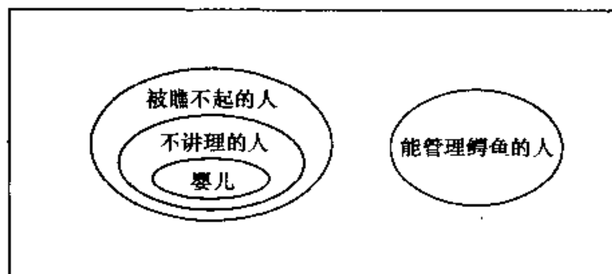


图 1-20

1.57 由三个前提得到 Venn 图,如图 1-21. 由此图得到结论(a)和(b)为真. 而结论(c)错误,因为可能存在非字典的有用的书.

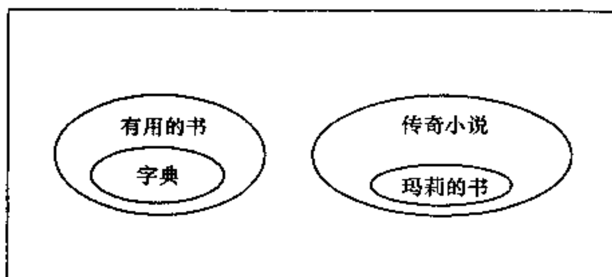


图 1-21

1.62 (a) $\{1,2,3,7,8,9\}$; (b) $\{1,3,4,6,8\}$; (c) $\{2,3,4,6\}$; (d) $\{2,3,4,6\}$.
(注意(c)=(d).)

第二章 关 系

2.1 引 言

在数学和计算机科学中使用的许多关系比如"小于","平行于","子集"等等已经为读者所熟悉.实际上,这些关系是考虑在一个确定的次序下的成对的事物之间的某种联系存在与否.规范地,我们利用这些"有序偶"来给出关系的定义.

有三种关系在本书中将起重要作用,即(i)等价关系,(ii)序关系,(iii)函数关系.等价关系主要在本章研究.序关系在此处引入,将在第十四章中讨论.函数关系将在下一章研究.

如上所述,关系将由元素的有序偶(a,b)来定义,这里a作为第一元素,而b则是第二元素.特别地,

$$(a,b)=(c,d)$$

当且仅当$a=c$且$b=d$.于是,$(a,b)\neq(b,a)$,除非$a=b$.这与第一章关于集合的讨论不同,在那里交换元素的次序是无所谓的,比如$\{3,5\}=\{5,3\}$.

尽管矩阵将在第五章中讨论,但作为对关系的完整讨论,我们将在本章引入矩阵与关系的联系.但是对于不具备矩阵概念的读者,在首次阅读本章时,可以略去有关矩阵的节.

2.2 集合的积

考虑任意两个集合A,B.称所有有序偶(a,b)的集合为A,B的*积*或*笛卡儿积*,其中$a\in A$,$b\in B$.A,B的积记作$A\times B$,读作"A叉B".由定义,

$$A\times B=\{(a,b):a\in A\text{ 且 }b\in B\}.$$

我们也常将$A\times A$写为A^2.

例 2.1 $\mathbf{R}$表示实数集,因此$\mathbf{R}^2=\mathbf{R}\times\mathbf{R}$为全体有序实数偶的集合.如图2-1,对于将$\mathbf{R}^2$表示为平面上的点的集合,读者已经司空见惯.这里每个点P表示一个有序实数偶(a,b),反之亦然.过P的垂线和水平线分别与x轴,y轴交于a和b.$\mathbf{R}^2$常称为*笛卡儿平面*.

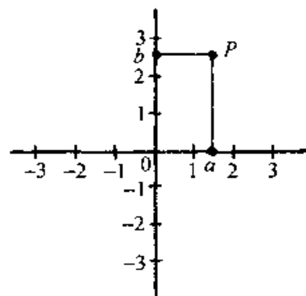


图 2-1

例 2.2 设$A=\{1,2\}$, $B=\{a,b,c\}$.则

$A\times B=\{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$,

$B\times A=\{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$.

且

$$A\times A=\{(1,1),(1,2),(2,1),(2,2)\}.$$

在上例中,有两点值得注意.首先,$A\times B\neq B\times A$.笛卡儿积由有序偶定义,构成积的集合的次序自然就十分重要.第二,记集合S中元素个数为$n(S)$,我们有

$$n(A\times B)=6=2\cdot 3=n(A)\cdot n(B).$$

事实上,对于任何的有限集A,B,均有$n(A\times B)=n(A)\cdot n(B)$.因为对于任意的有序偶$(a,b)$,元素$a$共有$n(A)$种可能选择,而对于$a$的每一个选择,$b$又都有$n(B)$种可能选择.

集合的积的概念可以推广到任意有限多个集合.对于任意的集合$A_1,A_2,\cdots,A_n$,称全体n元有序组$(a_1,a_2,\cdots,a_n)$的集合为$A_1,A_2,\cdots,A_n$的*积*,记作

$$A_1\times A_2\times\cdots\times A_n \quad\text{或}\quad \prod_{i=1}^{n}A_i,$$

其中,$a_1\in A_1,a_2\in A_2,\cdots,a_n\in A_n$.如同将$A\times A$记为$A^2$一样,我们也将$n$个$A$的积$A\times A\times\cdots\times A$记作$A^n$.例如,$\mathbf{R}^3=\mathbf{R}\times\mathbf{R}\times\mathbf{R}$即为通常的三维实数空间.

2.3 关 系

我们首先给出一个定义.

定义 设A,B为集合.$A\times B$的任一子集称为从A到B的一个二元关系或简称关系.

假定R是从A到B的一个关系.则R是一个有序偶的集合,在每个有序偶中,第一元素来自A而第二元素来自B.即对于每一对$a\in A$和$b\in B$,下列两种情况恰具其一:

(i) $(a,b)\in R$,称a与b之间具有关系R,记作aRb.

(ii) $(a,b)\notin R$,则a与b之间不具有关系R,记作$a\not R b$.

如果R是集合A到自身的一个关系,即R是$A^2=A\times A$的一个子集,则称R是A上的一个关系.

R的定义域是属于R的有序偶的第一元素的集合,而称所有第二元素的集合为R的值域.

涉及n元有序组的n元关系将在2.12中引入,此处在没有特别声明的前提下,关系一词总是指二元关系.

例 2.3 (a) 设$A=\{1,2,3\}$,$B=\{x,y,z\}$,且$R=\{(1,y),(1,z),(3,y)\}$.则R是$A\times B$的一个子集,因此R是从A到B的一个关系.相对于这个关系,

$$1Ry,\quad 1Rz,\quad 3Ry,\quad \text{但}\quad 1\not Rx,\quad 2\not Rx,\quad 2\not Ry,\quad 2\not Rz,\quad 3\not Rx,\quad 3\not Rz.$$

R的定义域为$\{1,3\}$,值域为$\{y,z\}$.

(b) 设$A=\{$鸡蛋,奶,玉米$\}$,$B=\{$奶牛,山羊,母鸡$\}$.我们可以定义由A到B的关系R为:$(a,b)\in R$如果a由b生产.即

$$R=\{(\text{鸡蛋},\text{母鸡}),(\text{奶},\text{奶牛}),(\text{奶},\text{山羊})\}.$$

相对于这个关系,

$$\text{鸡蛋}\ R\ \text{母鸡},\quad \text{奶}\ R\ \text{奶牛},\quad \text{等等}.$$

(c) 假定我们说两个国家相邻是指两个国家具有公共的国境线.那么,"相邻"就是世界上国家之间的一个关系R.于是

$$(\text{意大利},\text{瑞典})\in R,\quad \text{但是}\quad (\text{加拿大},\text{墨西哥})\notin R.$$

(d) 集合的包含$\subseteq$是集族上的一个关系.例如,任意给定一对集合A,B,则$A\subseteq B$或者$A\nsubseteq B$二者必具其一.

(e) 整数集合$\mathbf{Z}$上的一个为人熟知的关系是"m整除n".这个关系的通用记号为,当m整除n时,记$m|n$.于是,$6|30$而$7\nmid 25$.

(f) 考虑平面上直线的集合L.则垂直$\perp$是L上的一个关系.即任意给定一对直线a,b,则$a\perp b$或$a\not\perp b$二者必具其一.同样,平行于$\parallel$也是L上的一个关系,$a\parallel b$或者$a\nparallel b$二者必具其一.

(g) 设A为任一集合.A上的一个重要关系为相等.

$$\{(a,a):a\in A\}$$

通常记作"$=$".这个关系也称为集合A上的恒等或对角线关系,记作Δ_A或简记为Δ.

(h) 设A为任一集合.则$A\times A$和$\varnothing$都是$A\times A$的子集,因而也都是A上的关系,分别称为完全关系和空关系.

逆关系

设R为从集合A到B的任意一个关系.R的逆,记作R^{-1},是将R中的有序偶逆转后的有序偶的集合,是一个从B到A的关系.即

$$R^{-1}=\{(b,a):(a,b)\in R\}.$$

例如,从集合$A=\{1,2,3\}$到$B=\{x,y,z\}$的关系$R=\{(1,y),(1,z),(3,y)\}$的逆为

$$R^{-1} = \{(y,1),(z,1),(y,3)\}.$$

显然,如果 R 是一个关系,则$(R^{-1})^{-1}=R$. 同样地,R^{-1}的定义域和值域分别等于 R 的值域和定义域. 进而,若 R 是集合 A 上的一个关系,则 R^{-1}也是集合 A 上的一个关系.

2.4　关系的图示

我们首先来看实数集 $\mathbf{R}$ 上的一个关系 S,即 S 为 $\mathbf{R}^2=\mathbf{R}\times\mathbf{R}$ 的一个子集.

因为 $\mathbf{R}^2$ 可以表示为平面上的点的集合,我们可以通过标注平面上属于 S 的点来图示 S. 关系的图示有时也称为关系的图.

通常,一个关系由满足某给定方程

$$E(x,y) = 0$$

的有序实数偶构成. 我们通常将该关系与这个方程等同,称 $E(x,y)=0$ 为关系.

例 2.4　考虑由方程

$$x^2 + y^2 = 25$$

定义的关系 S. 即 S 由所有满足给定方程的有序实数偶(x,y)构成. 该方程的图像是以原点为圆心,5 为半径的圆,如图 2-2.

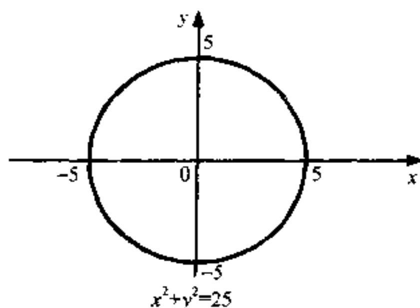


图 2-2

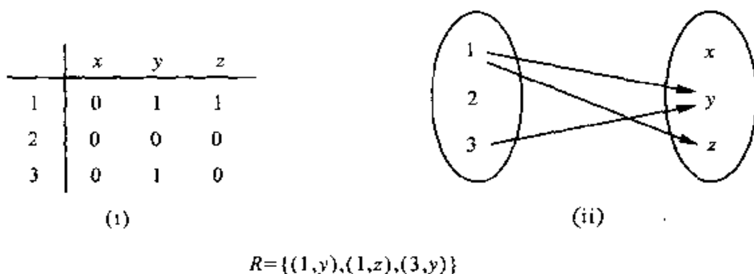
有限集上关系的图示

设 A,B 为有限集. 下面给出图示从 A 到 B 的关系 R 的两种方法.

(i) 构造一个矩阵,以 A 的元素和 B 的元素分别标注其行与列. 对于 $a\in A$ 和 $b\in B$,视 a,b 是否具有关系 R,在 a 行和 b 列交叉处标上 1 或 0. 这样得到的矩阵称为*关系矩阵*.

(ii) 在两个不交的碟形区域中分别写下 A 和 B 的元素. 当 a,b 具有关系 R 时,则画一个自 a 到 b 的箭头. 这样得到的图示称为关系的*箭头图*.

图 2-3 分别用两种方法图示了例 2.3 中的第一个关系.



	x	y	z
1	0	1	1
2	0	0	0
3	0	1	0

$R=\{(1,y),(1,z),(3,y)\}$

图 2-3

集上关系的有向图

当 R 为有限集到自身的关系时,可以用另一种方法给出 R 的图示. 我们首先写下给定集合的元素,对于每一个元素 x,如果 x 与元素 y 之间具有关系 R,我们就画一个自 x 到 y 的箭头. 这样得到的图形称为关系的*有向图*. 例如,图 2-4 即为集合 $A=\{1,2,3,4\}$上的关系

$$R = \{(1,2),(2,2),(2,4),(3,2),(3,4),(4,1),(4,3)\}$$

的有向图. 注意 2 与 2 具有关系 R,所以在图上有一个从 2 到自己的箭头.

有向图将在第八章中作为独立单元详细研究. 我们在这里提到它是为了完整说明其用途.

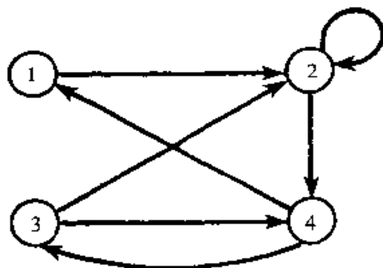


图 2-4

2.5 关系的合成

设 A,B,C 为集合，且 R 为从 A 到 B 的一个关系，S 为从 B 到 C 的一个关系. 即 R 为 $A\times B$ 的子集，S 为 $B\times C$ 的子集. 则由 R 和 S 决定了从 A 到 C 的一个关系，记作 $R\circ S$，定义为

$$a(R\circ S)c \text{ 如果对于某 } b\in B \text{ 我们有 } aRb \text{ 且 } bSc.$$

即

$$R\circ S=\{(a,c):\text{存在 } b\in B \text{ 使得}(a,b)\in R \text{ 且}(b,c)\in S\}.$$

关系 $R\circ S$ 称为 R 与 S 的合成，有时也简记为 RS.

设 R 为集合 A 上的一个关系，即 R 为 A 到自身的关系. 则 $R\circ R$ 为 R 与它自己的合成，有时记作 R^2. 类似地，$R^3=R^2\circ R=R\circ R\circ R$，等等. 由此，对于所有的正整数 n，我们可以定义 R^n.

注意 有些书籍将 R 与 S 的合成记为 $S\circ R$ 而不是 $R\circ S$. 因为对于函数 f 和 g，我们一般用 $g\circ f$ 表示 f 与 g 的复合，与此一致，就得到了关系的合成的上述记法. 在阅读参考书时，请读者注意其中的符号与本书的异同. 然而，当考虑一个关系 R 与自身的合成时，记号 $R\circ R$ 是不会产生混淆的.

如下例所示，关系的箭头图可以几何地直观描述合成 $R\circ S$.

例 2.5 设 $A=\{1,2,3,4\}$，$B=\{a,b,c,d\}$，$C=\{x,y,z\}$ 且

$$R=\{(1,a),(2,d),(3,a),(3,b),(3,d)\},$$
$$S=\{(b,x),(b,z),(c,y),(d,z)\}.$$

如图 2-5，考虑 R 与 S 的箭头图. 注意到有一个箭头从 2 到 d，继而又有一个箭头从 d 到 z. 我们可以把这两个箭头视为一条"连接" $2\in A$ 和 $z\in C$ 的"路". 于是，

$$\text{因为 } 2Rd \text{ 且 } dSz \text{ 所以 } 2(R\circ S)z.$$

类似地，从 3 到 x 和从 3 到 z 各有一条路，所以

$$3(R\circ S)x \quad \text{且} \quad 3(R\circ S)z.$$

再没有其他连接 A 与 C 的元素的路，所以

$$R\circ S=\{(2,z),(3,x),(3,z)\}.$$

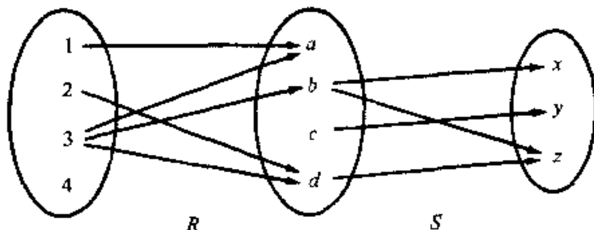


图 2-5

关系的合成与矩阵

这里介绍求 $R\circ S$ 的另一种方法. 设 M_R 和 M_S 分别表示关系 R 和 S 的矩阵. 则

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array} \quad 且 \quad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}.$$

将 M_R 与 M_S 相乘，得矩阵

$$M = M_R M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array}.$$

这个矩阵中的非零元素表示其所对应的元素具有关系 $R\circ S$. 于是，$M=M_RM_S$ 与 $M_{R\circ S}$的非零元素所处的位置相同.

下面的定理表明，关系的合成满足结合律.

定理 2.1 设 A,B,C,D 为集合. 假定 R 为从 A 到 B 的关系，S 为从 B 到 C 的关系，T 为从 C 到 D 的关系. 则

$$(R\circ S)\circ T = R\circ(S\circ T).$$

本定理的证明将在问题 2.11 中完成.

2.6 典型关系

给定集合 A. 本节讨论定义于集合 A 上的一些重要的典型关系.

自反关系

集合 A 上的关系 R 称为*自反的*，如果对于每个 $a\in A$，总有 aRa，即如果对每个 $a\in A$，$(a,a)\in R$. 因此，如果存在 $a\in A$，使得$(a,a)\notin R$，则 R 不是自反的.

例 2.6 设 $A=\{1,2,3,4\}$. 对于 A 上的如下关系：

$R_1=\{(1,1),(1,2),(2,3),(1,3),(4,4)\}$

$R_2=\{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$

$R_3=\{(1,3),(2,1)\}$

$R_4=\varnothing$，空关系

$R_5=A\times A$，全关系

试确定何者为自反关系.

因为 A 包含 4 个元素，所以如果 A 上的某关系 R 包含了四个有序偶$(1,1)$，$(2,2)$，$(3,3)$和$(4,4)$，则 R 为自反的. 于是上述只有 R_2 和全关系 $R_5=A\times A$ 为自反的. R_1，R_3 和 R_4 都不是自反的，比如$(2,2)$不属于其中的任一个.

例 2.7 对于下列五个关系，试判定何者为自反的.

(1) 整数集合 **Z** 上的关系$\leqslant$(小于等于关系).

(2) 集类 $\mathscr{C}$ 上的集合包含关系.

(3) 平面上直线的集合 L 上的关系$\perp$(垂直关系).

(4) 平面上直线的集合 L 上的关系$\parallel$(平行关系).

(5) 正整数集合 **N** 上的整除性关系$\mid$(注意，如果存在 z 使得 $xz=y$ 则 $x\mid y$).

关系(3)不是自反的，因为直线不与自身垂直. 同样，(4)不是自反的，因为直线不与自身平行. 其余关系都是自反的，即对 **Z** 中任意整数 x，有 $x\leqslant x$；对于 C 中任意集合 A，有 $A\subseteq A$；对于 **N** 中任意正整数 n，有 $n\mid n$.

对称和反对称关系

集合 A 上的关系 R 称为是**对称的**，如果由 aRb 必可推出 bRa，即只要 $(a,b)\in R$，则 $(b,a)\in R$. 于是，如果存在 $a,b\in R$，使得 $(a,b)\in R$ 但 $(b,a)\notin R$，则 R 不是对称的.

例 2.8 (a) 试确定例 2.6 中所列关系何者为对称的.

(b) 试确定例 2.7 中所列关系何者为对称的.

(a) R_1 不是对称的，因为 $(1,2)\in R_1$，但是 $(2,1)\notin R_1$. 又因为 $(1,3)\in R_3$ 但 $(3,1)\notin R_3$，所以 R_3 不是对称的. 其余关系都是对称的.

(b) 关系 $\perp$ 是对称的，因为若直线 $a\perp b$，则 $b\perp a$. 同样，因为若 $a\parallel b$，则 $b\parallel a$，所以平行关系也是对称的. 其余关系都不是对称的. 例如，$3\leqslant 4$ 但是 $4\nleqslant 3$；$\{1,2\}\subseteq\{1,2,3\}$，但是 $\{1,2,3\}\nsubseteq\{1,2\}$；$2|6$ 但是 $6\nmid 2$.

集合 A 上的关系 R 称为**反对称的**，如果 aRb 且 bRa 则必有 $a=b$. 即只要 $(a,b),(b,a)\in R$ 就有 $a=b$. 于是，如果存在 $a,b\in A$ 使得 (a,b) 与 (b,a) 都属于 R，但是 $a\neq b$，则 R 不是反对称的.

例 2.9 (a) 试确定例 2.6 中所列关系何者为反对称的.

(b) 试确定例 2.7 中所列关系何者为反对称的.

(a) R_2 不是反对称的，因为 $(1,2)$ 和 $(2,1)$ 都属于 R_1，但是 $1\neq 2$. 类似地，全关系 R_5 不是反对称的. 其余关系都是反对称的.

(b) 关系 $\leqslant$ 是反对称的，因为只要 $a\leqslant b$ 且 $b\leqslant a$，就必有 $a=b$. 集合的包含关系 $\subseteq$ 是反对称的，因为只要 $A\subseteq B$ 且 $B\subseteq A$，必有 $A=B$. 同样地，**N** 上的整除性关系是反对称的，因为只要 $m|n$ 且 $n|m$，就必有 $m=n$.（注意，整数集 **Z** 上的整除性关系不是反对称的，比如 $3|-3$ 且 $-3|3$，但是 $3\neq -3$.）$\perp$ 不是反对称的，因为 $a\perp b$ 且 $b\perp a$ 但 a,b 是相异直线. 同样地，$\parallel$ 也不是反对称的.

注 对称与反对称关系并不是互逆的. 例如，关系 $R=\{(1,3),(3,1),(2,3)\}$ 既不是对称的也不是反对称的. 另一方面，关系 $R'=\{(1,1),(2,2)\}$ 则既是对称的又是反对称的.

传递关系

集合 A 上的关系 R 称为是**传递的**，如果 aRb 且 bRc，则有 aRc，即只要 $(a,b),(a,c)\in R$，就必有 $(a,c)\in R$. 于是，如果存在 $a,b,c\in A$ 使得 $(a,b),(b,c)\in R$，但 $(a,c)\notin R$，则 R 不是传递的.

例 2.10 (a) 试确定例 2.6 中所列关系何者为传递的.

(b) 试确定例 2.7 中所列关系何者为传递的.

(a) R_3 不是传递的，因为 $(2,1),(1,3)\in R_3$ 但是 $(2,3)\notin R_3$. 其余关系都是传递的.

(b) 关系 $\leqslant,\subseteq,|$ 是传递的. 即(i) 若 $a\leqslant b,b\leqslant c$，则 $a\leqslant c$. (ii) 若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$. (iii) 若 $a|b$ 且 $b|c$，则 $a|c$.

另一方面，$\perp$ 不是传递的，因为由 $a\perp b,b\perp c$ 不能推出 $a\perp c$. 因为任何直线不与自身平行，故由 $a\parallel b,b\parallel a$，而 $a\nparallel a$ 知，平行关系 $\parallel$ 不是传递的.（注意，平面上直线集合 L 上的“平行且等于”是传递关系.）

关系的传递性质可以利用关系的合成来描述. 对于 A 上的一个关系 R，定义

$$R^2=R\circ R$$

更一般地，

$$R^n=R^{n-1}\circ R.$$

我们有下列结论.

定理 2.2 一个关系 R 是传递的当且仅当对于 $n\geqslant 1$ 有 $R^n\subseteq R$.

2.7 闭包性质

对于给定的集合 A，考虑其上所有关系构成的集族. 设 $\mathscr{P}$ 为这些关系的一个性质，比如对称或者传递等等. 我们将具有性质 $\mathscr{P}$ 的关系称为一个 $\mathscr{P}$-关系. 集合 A 上关系 R 的 $\mathscr{P}$-闭包是一个 $\mathscr{P}$-关系，满足对每个包含 R 的 $\mathscr{P}$-关系 S 有

$$R \subseteq \mathscr{P}(R) \subseteq S.$$

R 的 $\mathscr{P}$-闭包记作 $\mathscr{P}(R)$. 对于自反，对称，传递关系 R，记

$$\text{reflexive}(R), \quad \text{symmetric}(R), \quad \text{transitive}(R)$$

分别表示其闭包.

一般地，$\mathscr{P}(R)$ 未必存在. 但是，在某些条件下，$\mathscr{P}(R)$ 总是存在的. 假设 $\mathscr{P}$ 是一个性质，至少存在一个包含 R 的 $\mathscr{P}$-关系，而且任意 $\mathscr{P}$-关系的交仍然是一个 $\mathscr{P}$-关系. 则可以证明(问题 2.16)

$$\mathscr{P}(R) = \bigcap \{S : S \text{ 是 } \mathscr{P}\text{-关系，且 } R \subseteq S\}.$$

于是，我们可以由“下降法”来求得 $\mathscr{P}(R)$，即利用关系的交. 但是通常我们希望通过“上升法”来求 $\mathscr{P}(R)$，即在 R 中添加元素以获得 $\mathscr{P}(R)$. 下面我们讨论这种方法.

自反闭包和对称闭包

下面的定理告诉我们如何简易地求得一个关系的自反闭包和对称闭包. 记 $\Delta_A = \{(a,a) : a \in A\}$ 表示 A 上的对角线或恒等关系.

定理 2.3 设 R 为集合 A 上的一个关系. 则

(i) $R \cup \Delta_A$ 为 R 的自反闭包.

(ii) $R \cup R^{-1}$ 为 R 的对称闭包.

换句话说，reflexive(R) 可以通过在 R 中简单地添加那些不属于 R 的对角线元素 (a,a) 而得，为求得 symmetric(R)，只要对每个属于 R 的有序偶 (a,b)，在 R 中添加有序偶 (b,a).

例 2.11 (a) 考虑集合 $A = \{1,2,3,4\}$ 上的关系

$$R = \{(1,1),(1,3),(2,4),(3,1),(3,3),(4,3)\}.$$

则

$$\text{reflexive}(R) = R \cup \{(2,2),(4,4)\}, \quad \text{symmetric}(R) = R \cup \{(4,2),(3,4)\}.$$

(b) 考虑正整数集合 $\mathbf{N}$ 上的关系 $<$ (小于). 则

$$\text{reflexive}(<) = < \cup \Delta = \leqslant = \{(a,b) : a \leqslant b\},$$
$$\text{symmetric}(<) = < \cup > = \{(a,b) : a \neq b\}.$$

传递闭包

设 R 为集合 A 上的一个关系. 回忆 $R^2 = R \circ R$ 以及 $R^n = R^{n-1} \circ R$. 定义

$$R^* = \bigcup_{i=1}^{\infty} R^i.$$

下列定理成立.

定理 2.4 R^* 是关系 R 的传递闭包.

设 A 为含有 n 个元素的有限集. 我们在第九章讨论有向图时将证明

$$R^* = R \cup R^2 \cup \cdots \cup R^n.$$

由此可得下面的结果.

定理 2.5 设 R 为含 n 个元素的有限集 A 上的一个关系. 则

$$\text{transitive}(R) = R \cup R^2 \cup \cdots \cup R^n.$$

当 A 的元素个数很多时，求 transitive(R) 需要大量的时间. 在第八章中将给出一个有效的方法. 这里我们举一个简单的例子，其中 A 只有 3 个元素.

例 2.12 考虑集合 $A=\{1,2,3\}$ 上的关系

$$R=\{(1,2),(2,3),(3,3)\}.$$

则

$$R^2=R\circ R=\{(1,3),(2,3),(3,3)\},\quad R^3=R^2\circ R=\{(1,3),(2,3),(3,3)\}.$$

由此，

$$\text{transitive}(R)=R\cup R^2\cup R^3=\{(1,2),(2,3),(3,3),(1,3)\}.$$

2.8 等价关系

设 S 为非空集合. S 上的关系 R 称为一个等价关系，如果 R 是自反的，对称的和传递的. 即 S 上的关系 R 称为等价关系，如果 R 具有下列三条性质：

(1) 对每个 $a\in S$，有 aRa.

(2) 如果 aRb，则 bRa.

(3) 如果 aRb 且 bRc，则 aRc.

等价关系的另一层涵义是，它是集合中元素的一个分类，在同一类中的元素在某种意义上是"一样的". 事实上，任意集合上的元素之间的相等关系"="就是一个等价关系. 即

(1) 对每个 $a\in S$，有 $a=a$.

(2) 如果 $a=b$，则 $b=a$.

(3) 如果 $a=b$ 且 $b=c$，则 $a=c$.

下面的例子给出另外一些等价关系.

例 2.13 (a) 考虑欧氏平面上直线的集合 L 与三角形的集合 T. 则"平行或恒同"是 L 上的一个等价关系. 而全等与相似均为 T 上的等价关系.

(b) 以物种来给动物分类，即"属于同一种"的关系，是所有动物集合上的一个等价关系.

(c) 集合的包含关系 $\subseteq$ 不是一个等价关系. 它是自反的和传递的，但不是对称的. 因为显然 $A\subseteq B$ 并不意味着 $B\subseteq A$.

(d) 设 m 为一个取定的正整数. 两个整数 a 和 b 称为是模 m 同余的，记作

$$a\equiv b(\text{mod } m).$$

如果 m 能够整除 $a-b$. 例如，对于 $m=4$，我们有 $11\equiv 3(\text{mod } 4)$，因为 4 能够整除 $11-3$；$22\equiv 6(\text{mod } 4)$，因为 4 能整除 $22-6$. 模 m 同余是一个等价关系.

等价关系与集合的划分

本节研究非空集合 S 上的等价关系与划分之间的关系. 首先我们回忆集合 S 的划分 P 是由 S 的非空子集构成的集族 $\{A_i\}$，满足下面两个性质

(1) 每个 $a\in S$ 属于某个 A_i.

(2) 若 $A_i\neq A_j$，则 $A_i\cap A_j=\varnothing$.

换句话说，划分 P 将 S 剖分为不交的非空子集族(见 1.9).

假定 R 是集合 S 上的一个等价关系. 对于每个 $a\in S$，设 $[a]$ 表示与 a 具有关系 R 的 S 中元素的集合. 即

$$[a]=\{x:(a,x)\in R\}.$$

我们称 $[a]$ 为元素 a 在 S 中的等价类. 任意 $b\in[a]$ 称为该等价类的代表.

在关系 R 下，集合 S 的所有元素的等价类构成的集族记作 S/R，即

$$S/R=\{[a]:a\in S\}$$

称为 S 关于 R 的商集. 商集的基本性质由下面的定理给出.

定理 2.6 设 R 是集合 S 上的一个等价关系. 则商集 S/R 是 S 的一个划分. 特别地，

(i) 对于每个 $a\in S$，有 $a\in[a]$.

(ii) $[a]=[b]$当且仅当$(a,b)\in R$.

(iii) 若$[a]\neq[b]$,则$[a]$与$[b]$不交.

反之,给定集合 S 的一个划分$\{A_i\}$,则存在 S 上的一个等价关系 R,使得 A_i 是关于 R 的等价类.

这一重要定理将在问题 2.21 中给出证明.

例 2.14 (a) 考虑集合 $S=\{1,2,3\}$上的关系

$$R=\{(1,1),(1,2),(2,1),(3,3)\}.$$

可以证明 R 是自反的,对称的和传递的,即 R 是等价关系. 在 R 下,

$$[1]=\{1,2\},\quad [2]=\{1,2\},\quad [3]=\{3\}.$$

注意到$[1]=[2]$,所以 $S/R=\{[1],[3]\}$为 S 的一个划分. 我们可以任取$\{1,3\}$或$\{2,3\}$作为等价类的代表.

(b) 设 R_5 为整数集$\{Z\}$上由

$$x\equiv y(\text{mod }5)$$

定义的关系,读作"x 与 y 模 5 同余",即差 $x-y$ 可以被 5 整除. 于是 R_5 是集合 Z 上的一个等价关系. 在商集 Z/R_5 中恰有 5 个等价类,如下:

$$A_0=\{\cdots,-10,-5,0,5,10,\cdots\},$$
$$A_1=\{\cdots,-9,-4,1,6,11,\cdots\},$$
$$A_2=\{\cdots,-8,-3,2,7,12,\cdots\},$$
$$A_3=\{\cdots,-7,-2,3,8,13,\cdots\},$$
$$A_4=\{\cdots,-6,-1,4,9,14,\cdots\}.$$

注意到对于任意的整数 x,我们都可以用统一的格式 $x=5q+r(0\leqslant r<5)$来处理,x 属于等价类 A_r,其中 r 为余数. 显然,等价类是不交的,且

$$\mathbf{Z}=A_0\cup A_1\cup A_2\cup A_3\cup A_4.$$

通常我们取$\{0,1,2,3,4\}$或$\{-2,-1,0,1,2\}$作为等价类的代表.

2.9 偏序关系

本节定义另一类重要关系. 集合 S 上的一个关系 R 称为一个偏序,如果 R 是自反的,反对称的和可传递的. 集合 S 与偏序关系 R 一起,称为一个偏序集. 偏序集将在第于四章中详细讨论,这里仅给出一些例子.

例 2.15 (a) 对于任意的集族,集合的包含关系$\subseteq$是一个偏序,因为此关系满足偏序要求的三个性质. 即

(1) 对于任意的集合 A, $A\subseteq A$.

(2) 如果 $A\subseteq B$ 且 $B\subseteq A$,则 $A=B$.

(3) 如果 $A\subseteq B$ 且 $B\subseteq C$,则 $A\subseteq C$.

(b) 实数集 $\mathbf{R}$ 上的关系$\leqslant$满足自反,反对称和可传递性质,因此$\leqslant$是一个偏序.

(c) 关系"a 整除 b"是正整数集 $\mathbf{N}$ 上的一个偏序,但不是整数集 $\mathbf{Z}$ 上的偏序,因为在 $\mathbf{Z}$ 中,由 $a|b$ 且 $b|a$ 不能推出 $a=b$. 比如 $3|-3$ 且 $-3|3$,但 $3\neq-3$.

2.10 *n* 元关系

以上我们讨论的都是二元关系. 所谓 *n* 元关系,是指一个 n 元有序组的集合. 对于任意的集合 S,积集 S^n 的子集称为 S 上的一个 n 元关系. 特别,S^3 的子集称为 S 上的三元关系.

例 2.16 (a) 设 L 为平面上的一条直线. 则"介于"关系 R 是 L 上的点的集合上的一个三元关系,即如果 b 在 L 上介于 a 和 c 之间,则$(a,b,c)\in R$.

(b) 方程 $x^2+y^2+z^2=1$ 决定了实数集 $\mathbf{R}$ 上的一个三元关系 T. 即如果(x,y,z)满足上述方程,则三元数组(x,y,z)属于 T. 该方程表示(x,y,z)在 $\mathbf{R}^3$ 中以$(0,0,0)$为

圆心,1 为半径的球面.

问题与解答

有序偶与集合的积

2.1 给定 $A=\{1,2,3\}$ 及 $B=\{a,b\}$. 求:(a) $A\times B$; (b) $B\times A$; (c) $B\times B$.

解 (a) $A\times B$ 由所有有序偶(x,y)构成,其中 $x\in A, y\in B$. 因此

$$A\times B=\{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}.$$

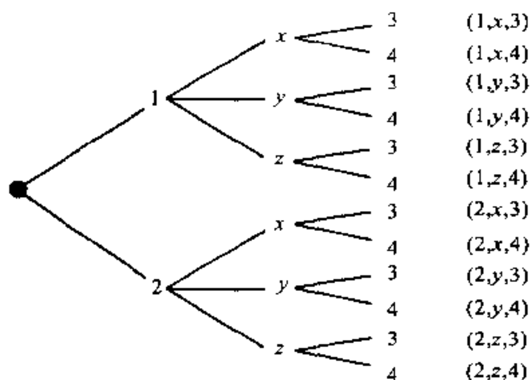
(b) $B\times A$ 由所有有序偶(y,x)构成,其中 $y\in B, x\in A$. 因此

$$B\times A=\{(a,1),(b,1),(a,2),(b,2),(a,3),(b,3)\}.$$

(c) $B\times B$ 由所有有序偶(x,y)构成,其中 $x,y\in B$. 因此

$$B\times B=\{(a,a),(a,b),(b,a),(b,b)\}.$$

如上所知,集合的积的元素个数正好等于各因子的元素个数的积.



(1,x,3)
(1,x,4)
(1,y,3)
(1,y,4)
(1,z,3)
(1,z,4)
(2,x,3)
(2,x,4)
(2,y,3)
(2,y,4)
(2,z,3)
(2,z,4)

图 2-6

2.2 给定 $A=\{1,2\}, B=\{x,y,z\}$ 及 $C=\{3,4\}$. 求:$A\times B\times C$.

解 $A\times B\times C$ 由所有三元有序组(a,b,c)构成,其中 $a\in A, b\in B, c\in C$. $A\times B\times C$ 的这些元素可以利用树图的方法系统地得到(如图 2-6). 在树图的右边,恰好得到 $A\times B\times C$ 的 12 个有序三元组. 注意到,$n(A)=2, n(B)=3, n(C)=2$,我们有

$$n(A\times B\times C)=12=n(A)\cdot n(B)\cdot n(C).$$

2.3 设 $A=\{1,2\}, B=\{a,b,c\}, C=\{c,d\}$. 求:$(A\times B)\cap(A\times C)$及 $A\times(B\cap C)$.

解 我们有

$$A\times B=\{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\},$$
$$A\times C=\{(1,c),(1,d),(2,c),(2,d)\}.$$

所以,

$$(A\times B)\cap(A\times C)=\{(1,c),(2,c)\}.$$

因为 $B\cap C=\{c\}$,所以

$$A\times(B\cap C)=\{(1,c),(2,c)\}.$$

我们看到$(A\times B)\cap(A\times C)=A\times(B\cap C)$. 事实上,这对于任意的集合 A,B,C 都成立(见问题 2.4).

2.4 证明:$(A\times B)\cap(A\times C)=A\times(B\cap C)$.

证
$$\begin{aligned}(A\times B)\cap(A\times C)&=\{(x,y):(x,y)\in A\times B \text{ 且 } (x,y)\in A\times C\}\\&=\{(x,y):x\in A, y\in B \text{ 且 } x\in A, y\in C\}\\&=\{(x,y):x\in A,\ y\in B\cap C\}\\&=A\times(B\cap C).\end{aligned}$$

2.5 给定$(2x,x+y)=(6,2)$. 求 x,y.

解 两个有序偶相等当且仅当其对应分量相等. 从而我们有方程

$$2x = 6, x + y = 2.$$

由此得到 $x=3, y=-1$.

关系及其图示

2.6 求从 $A=\{a,b,c\}$ 到 $B=\{1,2\}$ 的关系的个数.

解 ☞ 因为 $A\times B$ 共有 $3(2)=6$ 个元素，故 $A\times B$ 共有 $m=2^6=64$ 个子集. 于是共有 $m=64$ 个从 A 到 B 的关系.

2.7 给定 $A=\{1,2,3,4\}$，$B=\{x,y,z\}$. 设 R 为如下的从 A 到 B 的关系：

$$R = \{(1,y),(1,z),(3,y),(4,x),(4,z)\}.$$

(a) 求 R 的矩阵.

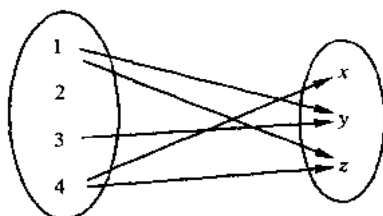
(b) 画出 R 的箭头图.

(c) 求 R 的逆关系 R^{-1}.

(d) 求 R 的定义域和值域.

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\begin{array}{c} \begin{array}{ccc} x & y & x \end{array} \\ \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \end{array}$$

(a)



(b)

图 2－7

解 ☞ (a) 如图 2－7(a). 注意其中矩阵的行由 A 的元素标出，而列由 B 的元素标出. 同样，对于 $a\in A, b\in B$，如果 a 与 b 有关系，则矩阵中的对应元素为 1，否则为 0.

(b) 见图 2－7(b). 注意，从 $a\in A$ 到 $b\in B$ 有一个箭头当且仅当 a 与 b 有关系，即 $(a,b)\in R$.

(c) 将 R 的有序偶逆转，则得到 R^{-1}：

$$R^{-1} = \{(y,1),(z,1),(y,3),(x,4),(z,4)\}.$$

将图 2－7(b)中的箭头逆转，则可得到 R^{-1} 的箭头图.

(d) R 的定义域 $\mathrm{Dom}(R)$，由 R 中的有序偶的第一元素构成，值域 $\mathrm{Ran}(R)$ 则由 R 中有序偶的第二元素构成. 于是

$$\mathrm{Dom}(R) = \{1,3,4\}, \quad \mathrm{Ran}(R) = \{x,y,z\}.$$

2.8 设 $A=\{1,2,3,4,6\}$，而 R 是 A 上的由"x 整除 y"定义的关系，记作 $x|y$.（注意 $x|y$ 当且仅当存在整数 z 使得 $xz=y$.）

(a) 将 R 写为有序偶的集合.

(b) 画出 R 的有向图.

(c) 求 R 的逆关系 R^{-1}. 问是否可以用语言来表述 R^{-1}？

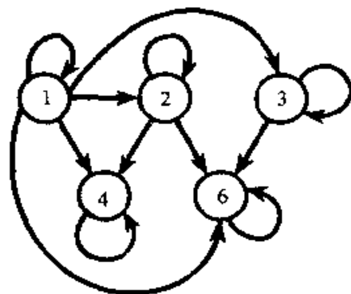


图 2－8

解 ☞ (a) 求出 A 中可以被 1,2,3,4,6 整除的元素即可. 我们有

$1|1,\ 1|2,\ 1|3,\ 1|4,\ 1|6,\ 2|2,\ 2|4,\ 2|6,\ 3|3,\ 3|6,\ 4|4,\ 6|6.$

所以

$R=\{(1,1),(1,2),(1,3),(1,4),(1,6),(2,2),(2,4),(2,6),(3,3),(3,6),(4,4),(6,6)\}.$

(b) 见图 2－8.

(c) 将 R 中的有序偶逆转即得 R^{-1}.

$R^{-1}=\{(1,1),(2,1),(3,1),(4,1),(6,1),(2,2),(4,2),(6,2),(3,3),(6,3),(4,4),(6,6)\}.$

R^{-1} 用语言描述即"x 是 y 的倍数".

2.9 设 $A=\{1,2,3\}$, $B=\{a,b,c\}$, $C=\{x,y,z\}$. 分别考虑下列从 A 到 B 的关系 R 和从 B 到 C 的关系 S.

$$R=\{(1,b),(2,a),(2,c)\},\quad S=\{(a,y),(b,x),(c,y),(c,z)\}.$$

(a) 求合成关系 $R\circ S$.

(b) 分别求关系 R, S 和 $R\circ S$ 的矩阵 M_R, M_S 和 $M_{R\circ S}$, 并将 $M_{R\circ S}$ 与 $M_R M_S$ 相比较.

解 (a)画出关系 R 和 S 的箭头图 2-9. 我们看到有一条路 $1\to b\to x$ 连接 A 中的元素 1 到 C 中的元素 x, 所以 $(1,x)$ 属于 $R\circ S$. 类似地, $(2,y)$, $(2,z)$ 属于 $R\circ S$. 我们有

$$R\circ S=\{(1,x),(2,y),(2,z)\}.$$

(见例 2.5).

(b) 矩阵 M_R, M_S 和 $M_{R\circ S}$ 如下:

$$M_R=\begin{array}{c}\\1\\2\\3\end{array}\begin{array}{c}\begin{array}{ccc}a&b&c\end{array}\\\begin{bmatrix}0&1&0\\1&0&1\\0&0&0\end{bmatrix}\end{array}\quad M_S=\begin{array}{c}\\a\\b\\c\end{array}\begin{array}{c}\begin{array}{ccc}x&y&z\end{array}\\\begin{bmatrix}0&1&0\\1&0&0\\0&1&1\end{bmatrix}\end{array}\quad M_{R\circ S}=\begin{array}{c}\\1\\2\\3\end{array}\begin{array}{c}\begin{array}{ccc}x&y&z\end{array}\\\begin{bmatrix}1&0&0\\0&1&1\\0&0&0\end{bmatrix}\end{array}.$$

将 M_R 与 M_S 相乘得到

$$\begin{bmatrix}1&0&0\\0&2&1\\0&0&0\end{bmatrix}.$$

考察 $M_{R\circ S}$ 与 $M_R M_S$, 我们看到, 它们的零元素的位置相同.

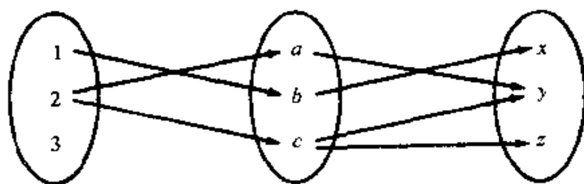


图 2-9

2.10 设集合 $A=\{1,2,3\}$ 上的关系 R 与 S 如下:

$$R=\{(1,1),(1,2),(2,3),(3,1),(3,3)\},\quad S=\{(1,2),(1,3),(2,1),(3,3)\}.$$

求: (a) $R\cap S$, $R\cup S$, R^c; (b) $R\circ S$; (c) $S^2=S\circ S$.

解 (a) 视 R 与 S 为集合, 取通常集合的交与并. 对于 R^c, 利用 $A\times A$ 为 A 上的全关系这一事实.

$R\cap S=\{(1,2),(3,3)\}$,

$R\cup S=\{(1,1),(1,2),(1,3),(2,1),(2,3),(3,1),(3,3)\}$,

$R^c=\{(1,3),(2,1),(2,2),(3,2)\}$.

(b) 对于每个有序偶 $(a,b)\in R$, 求出所有有序偶 $(b,c)\in S$, 则 $(a,c)\in R\circ S$. 例如, $(1,1)\in R$ 而 $(1,2)$, $(1,3)\in S$, 因此 $(1,2)$, $(1,3)$ 属于 $R\circ S$. 于是

$$R\circ S=\{(1,2),(1,3),(1,1),(2,3),(3,2),(3,3)\}.$$

(c) 仿照(b)中的算法, 我们有

$$S^2=S\circ S=\{(1,1),(1,3),(2,2),(2,3),(3,3)\}.$$

2.11 证明定理 2.1: 设 A, B, C, D 为集合. 假定 R 是从 A 到 B 的关系, S 是从 B 到 C 的关系, 而 T 是从 C 到 D 的关系. 则 $(R\circ S)\circ T=R\circ(S\circ T)$.

证 我们只要证明 $(R\circ S)\circ T$ 的每个有序偶都属于 $R\circ(S\circ T)$ 且反之亦然.

假定 (a,d) 属于 $(R\circ S)\circ T$. 则在 C 中存在 c 使得 $(a,c)\in R\circ S$ 且 $(c,d)\in T$. 因为 $(a,c)\in R\circ S$, 则在 B 中存在 b 使得 $(a,b)\in R$ 且 $(b,c)\in S$. 因为 $(b,c)\in S$ 且 $(c,d)\in T$, 我们有 $(b,d)\in S\circ T$, 又因为 $(a,b)\in R$ 和 $(b,d)\in S\circ T$, 我们有 $(a,d)\in R\circ(S\circ T)$. 于是 $(R\circ S)\circ T\subseteq R\circ(S\circ T)$. 类似地, $R\circ(S\circ T)\subseteq(R\circ S)\circ T$. 双方包含关系给出 $R\circ(S\circ T)=(R\circ S)\circ T$.

典型关系与闭包性质

2.12 考虑在集合 $A=\{1,2,3\}$ 上的下列五个关系：

$R=\{(1,1),(1,2),(1,3),(3,3)\}$,

$S=\{(1,1),(1,2),(2,1),(2,2),(3,3)\}$,

$T=\{(1,1),(1,2),(2,2),(2,3)\}$,

$\varnothing$=空关系,

$A\times A$=全关系.

判定上述关系中何者是:(a) 自反的;(b) 对称的;(c) 传递的;(d) 反对称的.

解☞ (a) R 不是自反的,因为 $2\in A$ 但 $(2,2)\notin R$. T 不是自反的,因为 $(3,3)\notin T$. 同样,$\varnothing$ 不是自反的. S 和 $A\times A$ 是自反的.

(b) R 不是对称的,因为 $(1,2)\in R$ 但 $(2,1)\notin R$,类似地,T 不是对称的. $S,\varnothing,A\times A$ 是对称的.

(c) T 不可传递,因为 $(1,2)$ 和 $(2,3)$ 属于 T 但 $(1,3)$ 不属于 T. 其余四个关系都是传递的.

(d) S 不是反对称的,因为 $1\neq 2$ 但 $(1,2),(2,1)$ 都属于 S. 类似地,$A\times A$ 不是反对称的.

2.13 给定集合 $A=\{1,2,3,4\}$. 考虑 A 上的下列关系：

$R=\{(1,1),(2,2),(2,3),(3,2),(4,2),(4,4)\}$.

(a) 画出 R 的有向图.

(b) 问 R 是否(i)自反,(ii)对称,(iii)传递,(iv)反对称?

(c) 求 $R^2=R\circ R$.

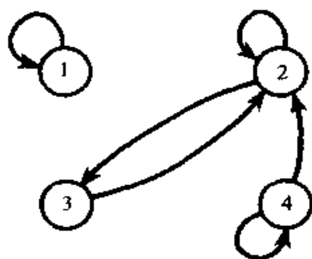


图 2-10

解☞ (a) 见图 2-10.

(b) (i) R 不是自反的,因 $3\in A$ 但 $3\not R 3$,即 $(3,3)\notin R$.

(ii) R 不是对称的,因 $4R2$ 但 $2\not R 4$,即 $(4,2)\in R$ 但是 $(2,4)\notin R$.

(iii) R 不是传递的,因 $4R2$ 且 $2R3$ 但 $4\not R 3$,即 $(4,2),(2,3)\in R$ 但 $(4,3)\notin R$.

(iv) R 不是反对称的,因 $2R3$ 且 $3R2$ 但 $2\neq 3$.

(c) 对于每一对 $(a,b)\in R$,求出所有 $(b,c)\in R$,则有 $(a,c)\in R^2$. 于是

$$R^2=\{(1,1),(2,2),(2,3),(3,2),(3,3),(4,2),(4,3),(4,4)\}.$$

2.14 请给出集合 $A=\{1,2,3\}$ 上的关系 R,使得 R 分别满足下列性质：

(a) R 既是对称的也是反对称的.

(b) R 既不是对称的也不是反对称的.

(c) R 是传递的,但是 $R\cup R^{-1}$ 不是传递的.

解☞ 对于每一个性质都可以列举出几个例子. 我们仅对每一性质给出一个例子：

(a) $R=\{(1,1),(2,2)\}$.

(b) $R=\{(1,2),(2,1),(2,3)\}$.

(c) $R=\{(1,2)\}$.

2.15 设 C 是集合 A 上的关系的族,而 T 是这族关系的交,即 $T=\bigcap(S:S\in C)$. 证明：

(a) 如果每个 S 都是对称的,则 T 也是对称的.

(b) 如果每个 S 都是传递的,则 T 也是传递的.

证☞ (a) 设 $(a,b)\in T$. 则对每个 S 有 $(a,b)\in S$. 因为每个 S 都是对称的,所以对每个 S 有 $(b,a)\in S$. 因此 $(b,a)\in T$,从而 T 是对称的.

(b) 设 $(a,b),(b,c)\in T$. 则 $(a,b),(b,c)$ 属于每个 S. 因为每个 S 都是传递的,所以对每个 S 有 $(a,c)\in S$. 因此 $(a,c)\in T$,从而 T 为传递的.

2.16 设 R 为集合 A 上的一个关系,并设 P 是关系的某个性质,如对称,传递等. 则称 P 为 R-可封闭的,如果 P 满足下列两个条件：

(1) 存在一个包含 R 的 P-关系 S.

(2) 所有 P-关系的交还是 P-关系.

(a) 证明:对任意的关系 R,对称性和传递性是 R-可封闭的.

(b) 设 P 是 R-可封闭的. 则 R 的 P-闭包 $P(R)$ 是所有包含 R 的 P-关系 S 的交,即

$$P(R)=\bigcap(S;S\text{ 是 }P\text{-关系,且 }R\subseteq S).$$

证 ☞ (a) 全关系 $A\times A$ 既是对称的也是传递的,而且包含 A 上的任何关系 R. 由问题 2.15,对称性和传递性满足(2). 于是,对于任意的关系 R,对称性和传递性是 R-可封闭的.

(b) 设 $T=\bigcap(S:S$ 是 P-关系,且 $R\subseteq S)$. 因为 P 是 R-可闭的,由(1),T 非空,由(2),T 是一个 P-关系. 由于每个关系 S 都包含 R,所以交集 T 包含 R. 即 T 是一个包含 R 的 P-关系. 由定义,$P(R)$ 是包含 R 的最小的 P-关系,因此 $P(R)\subseteq T$. 另一方面,$P(R)$ 是定义 T 的集合 S 中的一个,即 $P(R)$ 是一个 P-关系且 $R\subseteq P(R)$. 从而 $T\subseteq P(R)$. 于是 $P(R)=T$.

2.17 考虑集合 $A=\{a,b,c\}$ 及其上的关系

$$R=\{(a,a),(a,b),(b,c),(c,c)\}.$$

求:(a) reflexive(R); (b) symmetric(R); (c) transitive(R).

解 ☞ (a) R 的自反闭包可以由在 R 上添加不在其中的 $A\times A$ 的对角线元素得到. 因此,

$$\text{reflexive}(R)=R\cup\{(b,b)\}=\{(a,a),(a,b),(b,b),(b,c),(c,c)\}.$$

(b) R 的对称闭包可以由在 R 上添加不在其中的 R^{-1} 的元素获得. 因此,

$$\text{symmetric}(R)=R\cup\{(b,a),(c,b)\}=\{(a,a),(a,b),(b,a),(b,c),(c,b),(c,c)\}.$$

(c) 因为 A 具有三个元素,所以 R 的传递闭包可以由 R, $R^2=R\circ R$ 及 $R^3=R\circ R\circ R$ 的并集给出. 注意到

$$R^2=R\circ R=\{(a,a),(a,b),(a,c),(b,c),(c,c)\},$$
$$R^3=R\circ R\circ R=\{(a,a),(a,b),(a,c),(b,c),(c,c)\}.$$

于是

$$\text{transitive}(R)=R\cup R^2\cup R^3=\{(a,a),(a,b),(a,c),(b,c),(c,c)\}.$$

等价关系与划分

2.18 考虑整数集 $\mathbf{Z}$ 和整数 $m>1$. 我们说 x 与 y 模 m 同余,记作

$$x\equiv y(\text{mod }m).$$

如果 $x-y$ 可以被 m 整除. 证明由此定义的关系是 $\mathbf{Z}$ 上的一个等价关系.

证 ☞ 我们必须证明此关系是自反的,对称的,也是传递的.

(i) 对于 $\mathbf{Z}$ 中的每个 x 总有 $x-x=0$ 可以被 m 整除,故总有 $x\equiv x(\text{mod }m)$,所以该关系是自反的.

(ii) 假定 $x\equiv y(\text{mod }m)$,则 $x-y$ 可以被 m 整除. 从而 $-(x-y)=y-x$ 也可以被 m 整除,即 $y\equiv y(\text{mod }m)$. 于是,该关系是对称的.

(iii) 设 $x\equiv y(\text{mod }m)$, $y\equiv z(\text{mod }m)$,则 $x-y$ 与 $y-z$ 均可以被 m 整除. 则两者之和

$$(x-y)+(y-z)=x-z$$

也可以被 m 整除,从而 $x\equiv z(\text{mod }m)$. 于是该关系是传递的.

综上,整数集 $\mathbf{Z}$ 上模 m 同余关系是等价关系.

2.19 设 A 为非零整数的集合,$\approx$ 为 $A\times A$ 上的关系,定义为

$$(a,b)\approx(c,d)\quad\text{只要}\quad ad=bc.$$

证明 $\approx$ 是一个等价关系.

证 ☞ 我们必须证明 $\approx$ 是自反的,对称的,也是传递的.

(i) 自反性:因为 $ab=ba$,我们有 $(a,b)\approx(b,a)$. 所以 $\approx$ 是自反的.

(ii) 对称性:设 $(a,b)\approx(c,d)$. 则 $ad=bc$. 由此得 $cb=da$ 即 $(c,d)\approx(a,b)$. 于是 $\approx$ 是对称的.

(iii) 传递性:设 $(a,b)\approx(c,d)$ 且 $(c,d)\approx(e,f)$. 则 $ad=bc$ 且 $cf=de$. 将两边相乘,得 $(ad)(cf)=(bc)(de)$. 从两边消去 $c\neq0$ 和 $d\neq0$ 得到 $af=be$,因此 $(a,b)\approx(e,f)$. 于是 $\approx$ 为传递的.

综上,$\approx$ 是等价关系.

2.20 设已知集合 $A=\{1,2,3,4,5,6\}$ 上的等价关系

$R=\{(1,1),(1,5),(2,2),(2,3),(2,6),(3,2),(3,3),(3,6),(4,4),(5,1),(5,5),(6,2),(6,3),(6,6)\}$.

求 A 的由 R 诱导的划分,即求 R 的等价类.

解 ☞ 与 1 有关系的元素为 1 和 5,所以

$$[1]=\{1,5\}.$$

在 A 中取一个不属于[1]的元素,比如 2. 与 2 有关系的元素为 2,3,6,因此

$$[2]=\{2,3,6\}.$$

不属于[1]和[2]的元素只有 4,而与 4 有关系的元素也只有 4. 因此

$$[4]=\{4\}.$$

综上,由 R 确定的 A 的划分为

$$[\{1,5\},\{2,3,6\},\{4\}].$$

2.21 证明定理 2.6:设 R 为集合 A 上的等价关系. 则商集 A/R 为 A 的一个划分. 特别地,

(i) 对每个 $a\in A$,有 $a\in[a]$.

(ii) 仅当 $(a,b)\in R$ 时,有 $[a]=[b]$.

(iii) 如果 $[a]\neq[b]$,则 $[a]$ 与 $[b]$ 不交.

证 ☞ (i) 由于 R 是自反的,故对任意 $a\in A$ 有 $(a,a)\in R$,从而 $a\in[a]$.

(ii) 设 $(a,b)\in R$. 我们来证明 $[a]=[b]$. 设 $x\in[b]$. 则 $(b,x)\in R$. 但由假设有 $(a,b)\in R$,故由传递性得 $(a,x)\in R$,于是 $x\in[a]$. 由此,$[b]\subseteq[a]$. 为证明 $[a]\subseteq[b]$,注意到由 $(a,b)\in R$,据对称性可得 $(b,a)\in R$. 然后同理可证 $[a]\subseteq[b]$. 从而 $[a]=[b]$.

另一方面,如果 $[a]=[b]$,则由(i),$b\in[b]=[a]$,因此 $(a,b)\in R$.

(iii) 我们证明等价的逆否命题:

$$若[a]\cap[b]\neq\varnothing,则[a]=[b].$$

若 $[a]\cap[b]\neq\varnothing$,存在元素 $x\in A$ 满足 $x\in[a]\cap[b]$. 于是 $(a,x)\in R$ 且 $(b,x)\in R$. 由对称性,$(x,b)\in R$;由传递性,$(a,b)\in R$. 从而据(ii),$[a]=[b]$.

2.22 考虑单词的集合 $W=\{\text{sheet},\text{last},\text{sky},\text{wash},\text{wind},\text{sit}\}$. R 是由(a)"具有同样多的字母"或者(b)"具有相同的开头字母"定义的等价关系. 分别求由 R 确定的商集 W/R.

解 ☞ (a) 具有同样多字母的单词属于同一个单元,因此

$$W/R=[\{\text{sheet}\},\{\text{last},\text{wash},\text{wind}\},\{\text{sky},\text{sit}\}].$$

(b) 具有相同开头字母的单词属于同一个单元,因此

$$W/R=[\{\text{sheet},\text{sky},\text{sit}\},\{\text{last}\},\{\text{wash},\text{wind}\}].$$

偏序

2.23 设 $\mathscr{S}$ 为任一集族. 问集合的包含关系 $\subseteq$ 是否为 $\mathscr{S}$ 上的偏序?

解 ☞ 是. 因为集合的包含关系是自反的,反对称的和传递的. 也就是说,对于 $\mathscr{S}$ 中的任意集合 A,B,C,我们有:(i) $A\subseteq A$;(ii) 如果 $A\subseteq B$ 且 $B\subseteq A$,则 $A=B$;(iii) 如果 $A\subseteq B$ 且 $B\subseteq C$,则 $A\subseteq C$.

2.24 考虑整数集合 $\mathbf{Z}$. 对于某正整数 r,定义 aRb 如果 $b=a^r$. 证明 R 是 $\mathbf{Z}$ 上的一个偏序. 即证明 R 是:(a) 自反的;(b) 反对称的;(c) 传递的.

证 ☞ (a) R 是自反的,因为 $a=a^1$.

(b) 假设 aRb 且 bRa,其中 $b=a^r$,$a=b^s$. 则 $a=(a^r)^s=a^{rs}$. 这样共有四种可能性:(i) $rs=1$,(ii) $a=1$,(iii) $a=-1$. 如果 $rs=1$,则 $r=1$ 且 $s=1$,故 $a=b$. 如果 $a=1$,则 $b=1^r=1=a$. 类似地,若 $b=1$ 则 $a=1$. 最后,若 $a=-1$,则 $b=-1$(因为 $b\neq1$)且 $a=b$. 在这三种情况下,都有 $a=b$. 于是 R 是反对称的.

(c) 假定 aRb 且 bRc,其中 $b=a^r$ 且 $c=b^s$. 则 $c=(a^r)^s=a^{rs}$,于是 aRc. 即 R 是传递的.

综上 R 是 $\mathbf{Z}$ 上的一个偏序.

补 充 题

关系

2.25 设 $W=\{$玛克,艾利克,保罗$\}$而 $V=\{$艾利克,戴维$\}$. 求：(a) $W\times V$. (b) $V\times W$. (c) $V\times V$.

2.26 设 $S=\{a,b,c\}$, $T=\{b,c,d\}$, $W=\{a,d\}$. 试作出 $S\times T\times W$ 的树图,并求 $S\times T\times W$.

2.27 对于下列的条件

(a) $(x+2,4)=(5,2x+y)$;

(b) $(y-2,2x+1)=(x-1,y+2)$

分别求出 x,y.

2.28 证明：(a) $A\times(A\cap C)=(A\times B)\cap(A\times C)$;

(b) $A\times(B\cup C)=(A\times B)\cup(A\times C)$.

2.29 设 R 为集合 $A=\{1,2,3,4\}$上的下列关系：

$$R=\{(1,3),(1,4),(3,2),(3,3),(3,4)\}.$$

(a) 求 R 的矩阵 M_R.　　(b) 求 R 的定义域和值域.

(c) 求 R^{-1}.　　(d) 画出 R 的有向图.

(e) 求合成关系 $R\circ R$.

2.30 设集合 $B=\{a,b,c,d\}$上的关系 R 与 S 如下：

$$R=\{(a,a),(a,c),(c,b),(c,d),(d,b)\},$$

$$S=\{(b,a),(c,c),(c,d),(d,a)\}.$$

求下列合成关系：(a) $R\circ S$; (b) $S\circ R$; (c) $R\circ R$; (d) $S\circ S$.

2.31 设 R 为正整数集 **N** 上的一个由方程 $x+3y=12$ 定义的关系,即

$$R=\{(x,y):x+3y=12\}.$$

(a) 将 R 写为有序偶的集合.

(b) 求：(i) R 的定义域,(ii) R 的值域,(iii) R^{-1}.

(c) 求合成关系 $R\circ R$.

关系的性质

2.32 下述每个条件都定义了正整数集 **N** 上的一个关系.

(1) x 大于 y.　　(2) xy 为某整数的平方.

(3) $x+y=10$.　　(4) $x+4y=10$.

判定上述关系中何者为(a)自反的;(b)对称的;(c)反对称的;(d)传递的.

2.33 设 R,S 为集合 A 上的关系.假定 A 含有至少三个元素,判定下列是否正确. 如果不正确,请就集合 $A=\{1,2,3\}$给出反例.

(a) 如果 R 和 S 均为对称的,则 $R\cap S$ 也是对称的.

(b) 如果 R 和 S 均为对称的,则 $R\cup S$ 也是对称的.

(c) 如果 R 和 S 均为自反的,则 $R\cap S$ 也是自反的.

(d) 如果 R 和 S 均为自反的,则 $R\cup S$ 也是自反的.

(e) 如果 R 和 S 均为传递的,则 $R\cup S$ 也是传递的.

(f) 如果 R 与 S 均为反对称的,则 $R\cup S$ 也是反对称的.

(g) 如果 R 是反对称的,则 R^{-1} 也是反对称的.

(h) 如果 R 是自反的,则 $R\cap R^{-1}$ 非空.

(i) 如果 R 是对称的,则 $R\cap R^{-1}$ 非空.

2.34 设 R 与 S 是集合 A 上的关系,而且 R 是反对称的. 证明 $R\cap S$ 是反对称的.

等价关系

2.35 证明:如果 R 是集合 A 上的等价关系,则 R^{-1} 也是 A 上的一个等价关系.

2.36 设 $S=\{1,2,3,\cdots,19,20\}$. 令 R 是 S 上由 $x\equiv y(\mathrm{mod}5)$定义的等价关系,即 $x-y$ 可以被 5 整除. 求由 R 诱导的 S 的划分,即商集 S/R.

2.37 设 $A=\{1,2,3,\cdots,9\}$，并设～为 $A\times A$ 上的关系，定义为

$$(a,b)\sim(c,d) \quad 若 \quad a+d=b+c.$$

(a) 证明～是一个等价关系.

(b) 求[(2,5)]，即(2,5)的等价类.

补充题答案

2.25 (a) $W\times V=$ {(玛克，艾利克)，(玛克，戴维)，(艾利克，艾利克)，(艾利克，戴维)，(保罗，艾利克)，(保罗，戴维)}.

(b) $V\times W=$ {(艾利克，玛克)，(戴维，玛克)，(艾利克，艾利克)，(戴维，艾利克)，(艾利克，保罗)，(戴维，保罗)}.

(c) $V\times V=$ {(艾利克，艾利克)，(艾利克，戴维)，(戴维，艾利克)，(戴维，戴维)}.

2.26 $S\times T\times W$ 的树图，如图 2-11. 集合

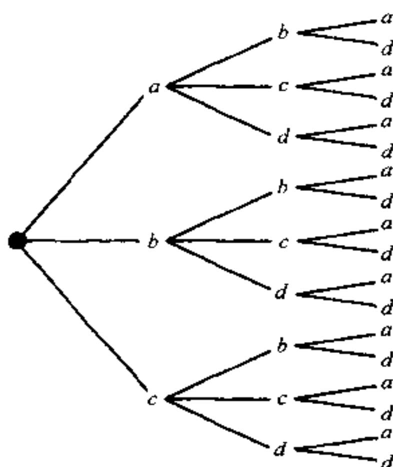


图 2-11

$$\begin{aligned}S\times T\times W=\{&(a,b,a),(a,b,d),(a,c,a),(a,c,d),(a,d,a),(a,d,d),\\&(b,b,a),(b,b,d),(b,c,a),(b,c,d),(b,d,a),(b,d,d),\\&(c,b,a),(c,b,d),(c,c,a),(c,c,d),(c,d,a),(c,d,d)\}.\end{aligned}$$

2.27 (a) $x=3,y=-2$； (b) $x=2,y=3$.

2.29 (a) $M_R=\begin{bmatrix}0&0&1&1\\0&0&0&0\\0&1&1&1\\0&0&0&0\end{bmatrix}$.

(b) 定义域 $=\{1,3\}$，值域 $=\{2,3,4\}$.

(c) $R^{-1}=\{(3,1),(4,1),(2,3),(3,3),(4,3)\}$.

(d) 见图 2-12.

(e) $R\circ R=\{(1,2),(1,3),(1,4),(3,2),(3,3),(3,4)\}$.

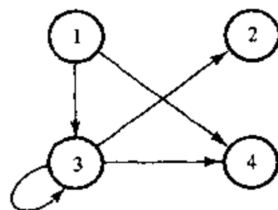


图 2-12

2.30 (a) $R\circ S=\{(a,c),(a,d),(c,a),(d,a)\}$.

(b) $S\circ R=\{(b,a),(b,c),(c,b),(c,d),(d,a),(d,c)\}$.

(c) $R\circ R=\{(a,a),(a,b),(a,c),(a,d),(c,b)\}$.

(d) $S\circ S=\{(c,c),(c,a),(c,d)\}$.

2.31 (a) $\{(9,1),(6,2),(3,3)\}$.

(b) (i) $\{9,6,3\}$，(ii) $\{1,2,3\}$，(iii) $\{(1,9),(2,6),(3,3)\}$.

(c) $\{(3,3)\}$.

2.32 (a) 无；(b) (2)和(3)；(c) (1)和(4)；(d) 除(3)以外.

2.33 除(e),(f)外全正确.对于(e),反例为 $R=\{(1,2)\}$,$S=\{(2,3)\}$.对于(f),反例为 $R=\{(1,2)\}$,$S=\{(2,1)\}$.

2.36 $[\{1,6,11,16\},\{2,7,12,17\},\{3,8,13,18\},\{4,9,14,19\},\{5,10,15,20\}]$.

2.37 (b) $\{(1,4),(2,5),(3,6),(4,7),(5,8),(6,9)\}$.

第三章 函数与算法

3.1 引 言

函数是数学中最重要的概念之一.术语"映射","变换"以及其他术语等等都具有同样的意义,在特定的场合中使用何种说法与各人的习惯和数学背景有关.

与函数有关的一个概念是算法.本章将给出算法的概念并讨论其复杂性.

3.2 函 数

假定对于集合 A 中的每个元素,我们都惟一地分配集合 B 的一个元素与之对应,这样的分配称为从 A 到 B 的函数.集合 A 称为此函数的定义域,集合 B 称为此函数的上域.

通常用记号来表示函数.如,设 f 表示从 A 到 B 的函数.则记

$$f:A\to B,$$

读作"f 为从 A 到 B 的函数"或者"f 将 A 映射到 B".如果 $a\in A$,则 $f(a)$(读作 a 的 f 像)表示由 f 分配给 a 的 B 中惟一的元素,称为 a 在 f 下的像值,或者 f 在 a 处的值.所有这些像值的集合称为 f 的值域或像.$f:A\to B$ 的像记作 $\mathrm{Ran}(f)$ 或 $\mathrm{Im}(f)$ 或 $f(A)$.

我们也常常用数学公式表示函数.例如,考虑一个将实数映射为其平方的函数,常以下列方式表示:

$$f(x)=x^2, \text{ 或 } x\mapsto x^2, \text{ 或 } \quad y=x^2.$$

在第一种表示中,x 称为变量,字母 f 表示函数.在第二种记号里,箭头$\mapsto$读作"变到".对于最后一种记号,由于 y 的取值依赖于 x 的取值,所以 x 称为自变量,y 称为因变量.

注 无论何时,当我们用公式给出变量 x 的函数时,如果没有特别说明,函数的定义域都是 $\mathbf{R}$(或者 $\mathbf{R}$ 的一个使得公式有意义的足够大的子集),并且上域也是 $\mathbf{R}$.

例 3.1 (a) 考虑函数 $f(x)=x^3$,即 f 将每个实数的立方分配给它.则 2 的像为 8,因此我们可以记 $f(2)=8$.

(b) 设 f 将世界上每个国家的首都分配给该国家.这里,f 的定义域为世界上的国家的集合,而上域为世界上的城市的集合.于是,法国的像为巴黎,换句话说,f(法国)=巴黎.

(c) 图 3-1 以直观的方法定义了一个从集合 $A=\{a,b,c,d\}$到集合 $B=\{r,s,t,u\}$的函数.这里

$$f(a)=s,\quad f(b)=u,\quad f(c)=r,\quad f(d)=s.$$

f 的像为像值的集合$\{r,s,u\}$.注意 t 不属于 f 的像,因为 t 不是任何元素在 f 下的像.

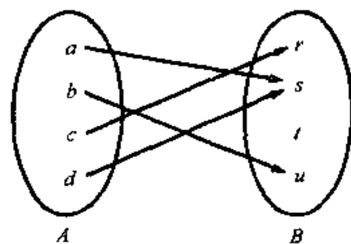


图 3-1

(d) 设 A 为任意集合.将 A 的每个元素分配为自身的从 A 到 A 的函数称为 A 上的恒同函数,通常记作 1_A 或简单地记为 1.换句话说,对于 A 中的每个元素 a,

$$1_A(a)=a.$$

(e) 假设 S 是 A 的一个子集,即 $S\subseteq A$.从 S 到 A 中的包含映射或嵌入,记作 $i:S\mapsto A$,为一个如下定义的函数:

$$i(x)=x,$$

对每个 $x\in S$.对于任意函数 $f:A\to B$,记 $f|_S$ 表示此函数在 S 上的限制,这是一个从 S 到 B 的函数,定义为

$$f|_S(x) = f(x),$$

对每个 $x \in S$.

函数与关系

我们介绍另一种处理函数的观点. 首先,每个函数 $f:A \to B$ 产生一个从 A 到 B 的关系,称为 f 的图,定义为

$$\text{图 } f = \{(a,b): a \in A, b = f(a)\}.$$

两个函数 $f:A \to B$ 与 $g:A \to B$ 称为相等,记作 $f=g$,如果对每个 $a \in A$ 有 $f(a)=g(a)$,也就是说,它们有相同的图. 因此,我们可以对一个函数与其图不作区分. 我们看到,在这样的图关系中,每一个 $a \in A$ 都属于其惟一的一个有序偶 (a,b). 另一方面,任何一个具有此性质的从 A 到 B 的关系 f 都给出了一个函数 $f:A \to B$,其中对 f 中的每个 (a,b),有 $f(a)=b$. 于是,我们可以给出函数的一个等价定义.

定义 3.1 函数 $f:A \to B$ 是一个从 A 到 B 的关系(即 $A \times B$ 的一个子集),使得每个 $a \in A$ 都属于 f 的惟一有序偶 (a,b).

尽管我们对于函数和它的图不作区分,但是当把 f 看做有序偶的集合时,我们仍然使用"f 的图"这一术语. 进而,因为 f 的图是一个关系,我们可以如研究关系时一样画出它的图形,称之为 f 的图像. 同时,f 的定义中,每个 $a \in A$ 都属于 f 的惟一有序偶的条件等价于任一条垂线与图像只有惟一交点的几何条件.

例 3.2 (a)设 $f:A \to B$ 为例 3.1(c)中所定义的函数. 则 f 的图是下列有序偶的集合.

$$\{(a,s),(b,u),(c,r),(d,s)\}.$$

(b) 考虑集合 $A=\{1,2,3\}$ 上的下列关系:

$f=\{(1,3),(2,3),(3,1)\}$,

$g=\{(1,2),(3,1)\}$,

$h=\{(1,3),(2,1),(1,2),(3,1)\}$.

f 是从 A 到 A 的函数,因为 A 的每一个元素作为 f 的有序偶的第一分量恰好出现一次,其中 $f(1)=3$, $f(2)=3$, $f(3)=1$. g 不是 A 到 A 的函数,因为不存在 g 的有序偶以 $2 \in A$ 作为第一分量,即 g 没有给 2 分配一个值. 同样地,h 不是 A 到 A 的函数,因为元素 $1 \in A$ 在 h 的两个相异有序偶(1,3)和(1,2)中都作为第一分量. 如果 h 是函数,则它不能对于元素 $1 \in A$ 同时分配两个不同的值 2 和 3.

(c) 所谓实多项式函数,是指形如

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

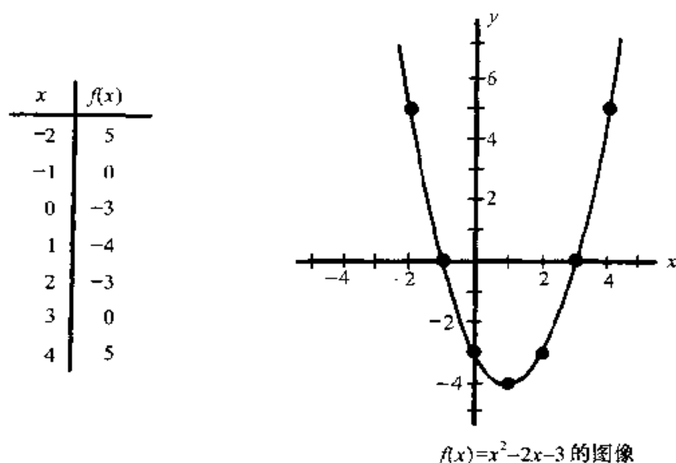
的函数 $f:\mathbf{R} \to \mathbf{R}$. 其中 a_i 都是实数. 因为 $\mathbf{R}$ 是无限集合,所以我们不可能图示该函数的每一点. 但是,我们可以首先作出这个函数的部分点,然后用光滑曲线将这些点连起来,从而得到该函数的近似的图示. 这些点可以通过由自变量 x 与其对应因变量 $f(x)$ 的取值构成的列表获得. 图 3-2 对于函数 $f(x)=x^2-2x-3$ 给出了这种方法的示例.

复合函数

考虑函数 $f: A \to B$ 和 $g: B \to C$,即 f 的上域就是 g 的定义域. 由此我们可以得到一个新的从 A 到 C 的函数,称为 f 与 g 的复合函数,记作 $g \circ f$,定义为

$$(g \circ f)(a) \equiv g(f(a)).$$

即我们首先求得元素 a 在 f 下的像,然后再求得 $f(a)$ 在 g 下的像. 这个概念实际上并不是新的. 如果我们把 f 与 g 看做关系,则复合函数也就是 f 与 g 的合成关系(见 2.6),不同之处是



x	$f(x)$
−2	5
−1	0
0	−3
1	−4
2	−3
3	0
4	5

图 3-2

复合函数的记号为 $g\circ f$ 而合成关系则记为 $f\circ g$.

对于任意的函数 $f: A\to B$,有

$$f\circ 1_A = f, \qquad 1_B\circ f = f.$$

其中 1_A 与 1_B 分别为 A,B 上的恒同函数.

3.3 一一的,映上的与可逆的函数

函数 $f: A\to B$ 称为一一的(记作 1-1),如果定义域 A 中的相异元素具有相异的像.换言之,称 f 是一一的,如果 $f(a)=f(a')$ 蕴含 $a=a'$.

一个函数 $f: A\to B$ 称为映上的,如果 B 的每个元素都是 A 的某个元素的像.换句话说,$f: A\to B$ 称为映上的,如果 f 的像为整个上域,即 $f(A)=B$.在这种情况下,我们说函数 f 是从 A 到 B 上的,或 f 将 A 映射到 B 上.

定理 3.1 函数 $f: A\to B$ 是可逆的当且仅当 f 既是一一的又是映上的.

如果函数 $f: A\to B$ 既是一一的又是映上的,则称 f 为 A 与 B 之间的一个一一对应.这个说法来自于下述事实,即 A 的每个元素对应于惟一一个 B 的元素,反之亦然.

有些教科书将一一的函数称为单射,将映上称为满射,而将一一对应称为双射.

例 3.3 考虑如图 3-3 定义的函数 $f_1: A\to B$,$f_2: B\to C$,$f_3: C\to D$ 及 $f_4: D\to E$.则 f_1 是一一的,因为 B 的任意一个元素都不是以上 A 的元素的像.类似地,f_2 也是一一的.但是 f_3 和 f_4 都不是一一的,因为 $f_3(r)=f_3(u)$,$f_4(v)=f_4(w)$.

考虑映上的情况,f_2 和 f_3 都是映上的,因为 C 的每个元素都是 B 的某个元素在 f_2 下的像,而 D 的每个元素都是 C 的某个元素在 f_3 下的像,即 $f_2(B)=C$,$f_3(C)=D$.另一方面,f_1 不是映上的,因为 $3\in B$ 不是 A 的任何元素在 f_1 下的像,f_4 也不是映上的,因为 $x\in E$ 不是 D 的任何元素在 f_4 下的像.

于是 f_1 是一一的,但不是映上的.f_3 是映上的但不是一一的.f_4 既不是一一的也不是映上的.而 f_2 既是一一的也是映上的,即是 B 与 C 之间的一个一一对应.因此 f_2 是可逆函数,且 f_2^{-1} 是一个自 C 到 B 的函数.

一一函数和映上函数的几何特征

因为函数可以等同于其图,而图是可以用图像画出的,我们自然要问,一一函数与映上函数是否具有几何意义.答案是肯定的.

说函数 $f: A\to B$ 是一一的,是指在 f 的图中不存在两个相异有序偶 (a_1,b) 和 (a_2,b).因

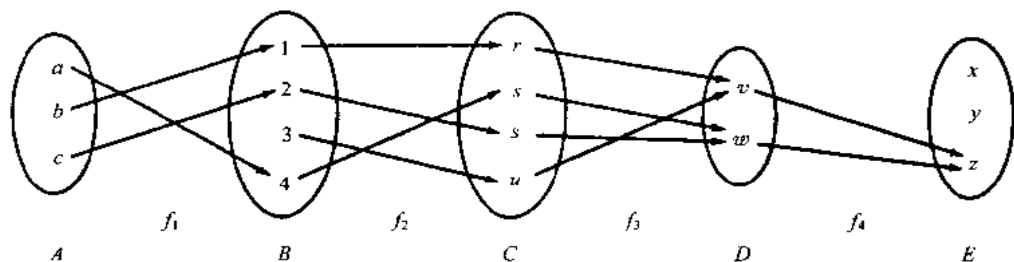


图 3-3

此每一条水平线至多与 f 的图像有一个交点. 另一方面,说函数 f 是映上的,是指对于每一个 $b\in B$,至少存在一个 $a\in A$ 使得(a,b)属于 f 的图. 因此,每一条垂线至少与 f 的图像有一个交点. 综上,如果 f 既是一一的又是映上的,即 f 为可逆函数,则每一条水平线与 f 的图像恰有一个交点.

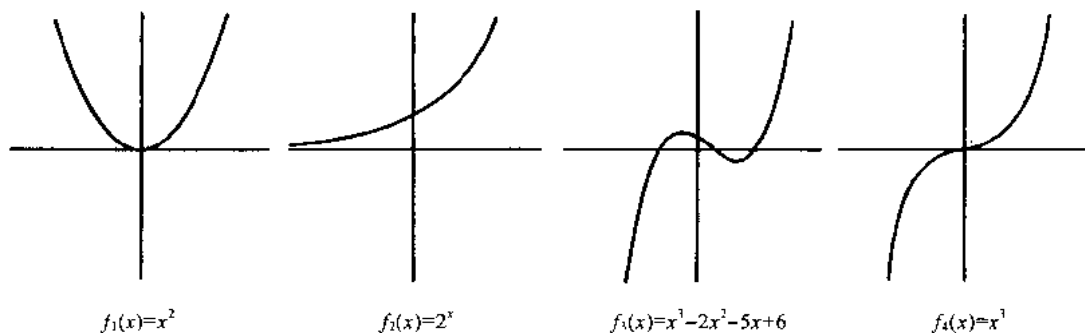


图 3-4

例 3.4　考虑下列四个从 **R** 到 **R** 的函数:

$$f_1(x)=x^2,\quad f_2(x)=2^x,\quad f_3(x)=x^3-2x^2-5x+6,\quad f_4(x)=x^3.$$

这些函数的图像如图 3-4. 对于 f_1,存在水平线与其图像交于两个点,也存在水平线与其图像不交,因此 f_1 既不是一一的也不是映上的. 类似地,可以看出 f_2 是一一的但非映上的,f_3 是映上的但不是一一的,f_4 既是一一的也是映上的. f_4 的逆函数是三次根式函数,即 $f_4^{-1}=\sqrt[3]{x}$.

3.4　数学函数,指数函数,对数函数

本节讨论算法分析和一般计算机科学中常见的数学函数及其记号,并讨论指数函数,对数函数及它们之间的关系.

上、下取整函数

设 x 为任意实数. 则 x 处于两个整数之间,称这两个整数为 x 的上取整和下取整. 特别地,

$\lfloor x\rfloor$称为 x 的下取整,表示小于 x 的最大整数.

$\lceil x\rceil$称为 x 的上取整,表示大于 x 的最小整数.

如果 x 为一个整数,则 $\lfloor x\rfloor=\lceil x\rceil$,否则 $\lfloor x\rfloor+1=\lceil x\rceil$. 例如,

$$\lfloor 3.14\rfloor=3,\quad \lfloor\sqrt{5}\rfloor=2,\quad \lfloor -8.5\rfloor=-9,\quad \lfloor 7\rfloor=7,\quad \lfloor -4\rfloor=-4;$$

$$\lceil 3.14\rceil=4,\quad \lceil\sqrt{5}\rceil=3,\quad \lceil -8.5\rceil=-8,\quad \lceil 7\rceil=7,\quad \lceil -4\rceil=-4.$$

取整函数和绝对值函数

设 x 为任意实数. x 的取整函数,记作 INT(x),由删去(截断)小数点后的部分将 x 变为

一个整数. 于是

$$\mathrm{INT}(3.14)=3,\quad \mathrm{INT}(\sqrt{5})=2,\quad \mathrm{INT}(-8.5)=-8,\quad \mathrm{INT}(7)=7.$$

注意到当 x 为正数时,有 $\mathrm{INT}(x)=\lfloor x\rfloor$;当 x 为负数时,$\mathrm{INT}(x)=\lceil x\rceil$.

实数 x 的绝对值记作 $\mathrm{ABS}(x)$或$|x|$,定义为 x 或 $-x$ 中较大者. 因此 $\mathrm{ABS}(0)=0$,而且对于 $x\neq0$,相应于 x 为正或负,有 $\mathrm{ABS}(x)=x$ 或 $\mathrm{ABS}(x)=-x$. 于是

$$|-15|=15,\ |7|=7,\ |-3.33|=3.33,\ |4.44|=4.44,\ |-0.075|=0.075.$$

注意到$|x|=|-x|$,而且,对于 $x\neq0$,$|x|$为正数.

余数函数与模算术

设 k 为任意整数,M 为一个正整数. 则

$$k(\mathrm{mod}\ M)$$

(读作 k 模M)为以 M 除 k 的整数余数. 确切地说,$k(\mathrm{mod}\ M)$是惟一的整数 r 满足

$$k=Mq+r\quad,\quad 0\leqslant r<M.$$

当 k 为正数时,直接以 M 除 k 得到余数 r. 于是

$$25(\mathrm{mod}7)=4,\ 25(\mathrm{mod}5)=0,\ 35(\mathrm{mod}11)=2,\ 3(\mathrm{mod}8)=3.$$

如果 k 为负数,则以 M 除$|k|$得到余数 r',然后若 $r'\neq0$, $k(\mathrm{mod}\ M)=M-r'$. 于是

$$-26(\mathrm{mod}7)=7-5=2,\ -371(\mathrm{mod}8)=8-3=5,\ -39(\mathrm{mod}3)=0.$$

"mod"术语也用于数学中的同余关系,定义如下:

$$a\equiv b(\mathrm{mod}\ M)\quad 当且仅当\quad M\ 整除\ b-a.$$

其中 M 称为模,而 $a\equiv b(\mathrm{mod}\ M)$读作"$a$ 与 b 模 M 同余". 以下的同余形式将常常用到.

$$0\equiv M(\mathrm{mod}\ M),\quad a\pm M\equiv a(\mathrm{mod}\ M).$$

模 M 算术,相对于加,减,乘等算术运算,在其中分别用集合

$$\{0,1,2,\cdots,M-1\}$$

或集合

$$\{1,2,3,\cdots,M\}$$

中的数来代替算术值. 例如,在模 12 的算术,有时也称为"时钟"算术中,

$$6+9\equiv3,\quad 7\times5\equiv11,\quad 1-5\equiv8,\quad 2+10\equiv0\equiv12.$$

(何时用 0,何时用 M 视具体应用情况而定).

指数函数

回忆下列整数指数(其中 m 为正整数)的定义

$$a^m=a\cdot a\cdots a(m\ 个\ a),\quad a^0=1,\quad a^{-m}=\frac{1}{a^m}.$$

由定义,指数可以拓展到所有有理数,对于任意的有理数 m/n,

$$a^{m/n}=\sqrt[n]{a^m}=(\sqrt[n]{a})^m.$$

例如,

$$2^4=16,\ 2^{-4}=\frac{1}{2^4}=\frac{1}{16},\ 125^{2/3}=5^2=25.$$

事实上,由定义,指数可以拓展为所有实数,对于任意实数 x,

$$a^x=\lim_{r\to x}a^r,$$

其中 r 为有理数. 由此,可以认为指数函数 $f(x)=a^x$ 的定义域为实数集.

对数函数

对数是与指数相关的函数. 设 b 为正数,任意正数 x 的以 b 为底的对数记作

$$\log_b x,$$

表示可以得到 x 的 b 的指数，即

$$y=\log_b x,\ b^y=x$$

是等价的. 因此，

由 $2^3=8$ 得，$\log_2 8=3$；　　由 $10^2=100$ 得，$\log_{10}100=2$；

由 $2^6=64$ 得，$\log_2 64=6$；　由 $10^{-3}=0.001$ 得，$\log_{10}0.001=-3$.

进而，对于任意的底 b，

因为 $b^0=1$，所以 $\log_b 1=0$.

因为 $b^1=b$，所以 $\log_b b=1$.

负数与 0 的对数没有定义.

对数通常用近似值给出. 例如，利用对数表或计算器，可以得到

$$\log_{10}300=2.4771,\quad \log_e 40=3.6889.$$

(其中 e=2.718281…).

三类重要的对数是：以 10 为底的对数，称为常用对数；以 e 为底的对数，称为自然对数；以 2 为底的对数，称为二进制对数. 有些教科书将 $\log_e x$ 记为 $\ln x$，将 $\log_2 x$ 记为 $\lg x$ 或 $\log x$. $\log x$ 通常表示 $\log_{10}x$，但是在高等数学课本中，它也被用来表示 $\log_e x$，而在计算机教科书中，又被用来表示 $\log_2 x$.

对于二进制对数，我们通常只需要它的上取整或下取整. 例如

因为 $2^6=64$，而 $2^7=128$，故 $\lfloor\log_2 100\rfloor=6$，

因为 $2^8=512$，而 $2^9=1024$，故 $\lceil\log_2 1000\rceil=9$，

等等.

指数函数与对数函数的关系

指数函数与对数函数，即

$$f(x)=b^x \quad 与 \quad g(x)=\log_b x$$

之间是互逆的关系，这两个函数的图形具有几何联系. 这个关系如图 3-5 所示，其中指数函数 $f(x)=2^x$，对数函数 $g(x)=\log_2 x$ 与线性函数 $h(x)=x$ 的图像画在同一个坐标系中. 因为 $f(x)=2^x$ 与 $g(x)=\log_2 x$ 为互逆的，所以它们关于线性函数 $h(x)=x$ 对称，换句话说，关于直线 $y=x$ 对称.

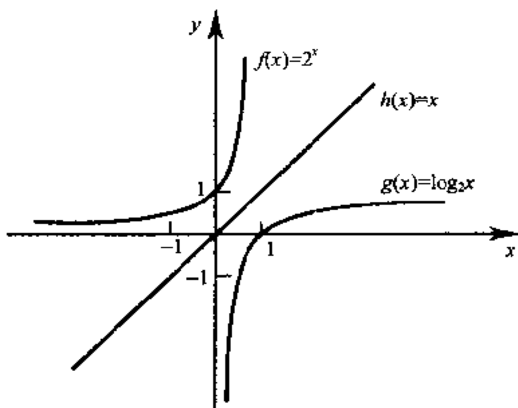


图 3-5

图 3-5 还表现了指数函数与对数函数的另一个重要性质. 特别地，对于任意的正数 c，我们有

$$g(c)<h(c)<f(c).$$

事实上，当 c 增大时，垂直距离 $h(c)-g(c)$ 和 $f(c)-g(c)$ 也增大. 进而，与线性函数 $h(x)$ 比较，

对数函数 $g(x)$ 上升较为缓慢,而指数函数 $f(x)$ 则上升较快.

3.5 序列,集合的指标类

序列和集合的指标类是具有其特定记号的特殊函数类型.本节将讨论这些函数,并讨论求和记号.

序列

*序列*是从正整数的集合 $\mathbf{N}=\{1,2,3,\cdots\}$ 到一个集合 A 的函数.我们用 a_n 表示整数 n 的像.于是序列通常表示为

$$a_1, a_2, a_3, \cdots \quad 或 \quad \{a_n : n \in \mathbf{N}\} \quad 或简记为 \quad \{a_n\}.$$

有时我们也以非负整数的集合 $\{0,1,2,\cdots\}$ 而非 $\mathbf{N}$ 作为序列的定义域.在这一情况下,我们说 n 从 0 开始而不是从 1 开始.

集合 A 上的*有限序列*是一个从 $\{1,2,\cdots,m\}$ 到 A 的函数,通常表示为

$$a_1, a_2, \cdots, a_m.$$

这样的有限序列有时也称为一个*列表*或 *m-元组*.

例 3.5 (a) 我们熟知的序列

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots \quad 与 \quad 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \cdots$$

可以分别规范地定义为

$$a_n = \frac{1}{n} \quad 与 \quad b_n = 2^{-n}.$$

其中第一序列由 $n=1$ 开始,而第二序列由 $n=0$ 开始.

(b) 重要序列 $1,-1,1,-1,\cdots$ 可以规范地定义为

$$a_n = (-1)^{n+1} \text{ 或等价地 } \quad b_n = (-1)^n.$$

其中第一序列由 $n=1$ 开始,而第二序列由 $n=0$ 开始.

(c) (串) 设集合 A 为有限集,并将 A 看指标集或字母集.则 A 上的一个有限序列称为一个*串*或*词*,通常记作 $a_1a_2\cdots a_m$,即不用括号.在串中的指标数 m 称为*长度*.指标为零时也看着一个串,称为*空串*或*零串*.我们将在第十三章中详细讨论一个字母表 A 上的串以及运算.

求和记号与求和

这里我们引入求和记号 $\sum$(希腊字母 sigma).考虑一个序列 $a_1, a_2, a_3, \cdots$,则和

$$a_1 + a_2 + \cdots + a_n \quad 与 \quad a_m + a_{m+1} + \cdots + a_n$$

将分别记作

$$\sum_{j=1}^{n} a_j \quad 与 \quad \sum_{j=m}^{n} a_j.$$

在上述表达式中,字母 j 称为*哑指标*或*哑变量*.其他字母如 i,k,s,t 等也常被用作哑变量.

例 3.6

$$\sum_{i=1}^{n} a_i b_i = a_1b_1 + a_2b_2 + \cdots + a_nb_n.$$

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 - 5^2 = 4 + 9 + 16 + 25 = 54.$$

$$\sum_{j=1}^{n} j = 1 + 2 + \cdots + n.$$

最后一个和式是最常见的,它的值为 $n(n+1)/2$.即

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

于是，

$$1+2+\cdots+50=\frac{50(51)}{2}=1275.$$

集合的指标类

设 I 为任意非空集合，并设 S 为集族. 从 I 到 S 的指标函数为一个函数 $f: I\to S$. 对于任意的 $i\in I$，记 A_i 表示其像 $f(i)$. 于是指标函数 f 通常表示为

$$\{A_i : i\in I\} \quad 或 \quad \{A_i\}_{i\in I} \quad 或简记为\{A_i\}.$$

集合 I 称为指标集，I 的元素称为指标. 如果 f 为一一的和映上的，我们就说 S 可以由 I 标出.

集合的指标类的并与交定义为

$$\bigcup_{i\in I}A_i=\{x : x\in A_i \ 对于某\ i\in I\} \quad 与 \quad \bigcap_{i\in I}A_i=\{x : x\in A_i \ 对所有\ i\in I\}.$$

如果 I 为有限集，则这恰好是我们以前定义的并和交. 如果 I 是 $\mathbf{N}$，我们可以分别定义并与交为

$$A_1\cup A_2\cup\cdots \quad 与 \quad A_1\cap A_2\cap\cdots.$$

例 3.7 设 I 为整数集 $\mathbf{Z}$. 对于每个整数 n，我们分配 $\mathbf{R}$ 的下列子集

$$A_n=\{x : x\leqslant n\}.$$

换言之，A_n 为无穷区间 $(-\infty, n]$. 对于每个实数 a，存在整数 n_1 和 n_2 使得 $n_1<a<n_2$，因此，$a\in A_{n_2}$ 但 $a\notin A_{n_1}$. 因此

$$a\in\bigcup_n A_n \quad 但 \quad a\notin\bigcap_n A_n.$$

由此

$$\bigcup_n A_n=\mathbf{R} \quad 但 \quad \bigcap_n A_n=\varnothing.$$

3.6 递归函数

一个函数称为是递归定义的，如果该函数的定义与其自身有关. 为了不至于产生循环定义，函数的递归定义必须具有下列两个性质：

(1) 必须存在一个称为基准值的叙述，不与函数自身相关.

(2) 在每一时刻函数都与自身相关，但函数的描述必须封闭于基准值. 具备这两个性质的递归函数称为良好定义的.

下面的例子有助于弄清这些概念.

阶乘函数

从 1 到 n 的所有正整数的积称为"n 阶乘"，通常记作 $n!$，即

$$n!=1\cdot 2\cdot 3\cdots(n-2)(n-1)n.$$

我们定义 $0!=1$，这样阶乘函数的定义就拓展了到全体非负整数. 于是我们有

$$0!=1,\ 1!=1,\ 2!=1\cdot 2=2,\ 3!=1\cdot 2\cdot 3=6,\ 4!=1\cdot 2\cdot 3\cdot 4=24,$$
$$5!=1\cdot 2\cdot 3\cdot 4\cdot 5=120,\quad 6!=1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6=720,$$

等等. 我们有

$$5!=5\cdot 4!=5\cdot 24=120,\quad 6!=6\cdot 5!=6\cdot 120=720.$$

这对任意正整数成立，即

$$n!=n\cdot(n-1)!.$$

由此，阶乘函数又可以给出如下定义.

定义 3.2 （阶乘函数） (1) 如果 $n=0$，则 $n!=1$.

(2) 如果 $n>0$，则 $n!=n\cdot(n-1)!$.

上述 $n!$ 的定义是递归的，因为当它使用 $(n-1)!$ 时，它与自身相关，然而

(1) 当 $n=0$ 时，$n!$ 的值已经明确地给出(于是 0 为一个基准值).

(2) 对于任意的 n，$n!$ 的值的定义利用了较小的 n 的阶乘值，而这个较小的 n 阶乘值封闭于基准值 0.

由此，这个定义不是循环的，换言之，阶乘函数是良好定义的.

例 3.8 我们利用递归定义来计算 4!. 这个计算需要下列九步：

(1) $4!=4\cdot 3!$

(2) $3!=3\cdot 2!$

(3) $2!=2\cdot 1!$

(4) $1!=1\cdot 0!$

(5) $0!=1$

(6) $1!=1\cdot 1=1$

(7) $2!=2\cdot 1=2$

(8) $3!=3\cdot 2=6$

(9) $4!=4\cdot 6=24$

即

第一步 利用 3! 定义 4!，所以必须 3! 有定义 4! 才能有定义. 这就促使我们进入下一步.

第二步 这里 3! 由 2! 定义，所以，要使 3! 有意义，必须使得 2! 有意义.

第三步 利用 1! 定义 2!.

第四步 利用 0! 定义 1!.

第五步 因为 0! 是递归定义的基准值，所以此步可以确切地确定 0!.

第六至九步 倒转回去，由 0! 求 1!，由 1! 求 2!，由 2! 求 3!，最后，由 3! 求出 4!. 倒转计算是由上述第一到第五步引导的.

注意，我们是由基准值起始倒转计算的.

水平数

设 P 为一个用来确定 $f(X)$ 的过程或者递归公式，其中 f 为递归函数，X 为输入值. 我们将 P 的每一步操作联系一个水平数. P 的原始操作步骤规定为水平 1；由于递归代入，P 的每一时刻的操作的水平数都比其递归代入的水平数增加 1. 递归的深度即为获得 $f(X)$ 的 P 的最大操作水平数.

比如，例 3.8 确定 4!，使用的递归公式为 $n!=n(n-1)!$. 第一步属于水平 1，因为它是递归公式的首次操作. 于是，

第二步属于水平 2，第三步属于水平 3，…，第五步属于水平 5.

另一方面，第六步属于水平 4，因为它是由水平 5 回代的结果. 换言之，第六步和第四步属于同一个操作水平. 类似地，

第七步属于水平 3，第八步属于水平 2，第九步属于水平 1.

由此，确定 4! 的递归深度为 5.

Fibonacci 序列

Fibonacci 序列(通常记作 $F_0, F_1, F_2, \cdots$)如下：

$$0,1,1,2,3,5,8,13,21,34,55,\cdots.$$

即 $F_0=0$，$F_1=1$，以后每一项都是其前面两项的和. 例如，上述序列将要列出的两项分别为

$$34+55=89, \quad 55+89=144.$$

这个函数的正式定义如下：

定义 3.3(Fibonacci 序列)　(a) 如果 $n=0$ 或 $n=1$，则 $F_n=n$.

(b) 如果 $n>1$，则 $F_n=F_{n-2}+F_{n-1}$.

这是另一个递归定义的例子，因为定义中用到了 F_{n-2} 和 F_{n-1}，所以该定义依赖了函数自身. 但是，

(1) 基准值为 0 和 1.

(2) F_n 的定义利用了比 n 小的函数值，而这些值封闭于基准值. 所以这个函数是良好定义的.

Ackermann 函数

Ackermann 函数是含有两个自变量的函数，每一个自变量的取值范围都是非负整数. 该函数的定义如下：

定义 3.4(Ackermann 函数)　(a) 如果 $m=0$，则 $A(m,n)=n+1$.

(b) 如果 $m\neq 0$ 但是 $n=0$，则 $A(m,n)=A(m-1,n)$.

(c) 如果 $m\neq 0$ 且 $n\neq 0$，则 $A(m,n)=A(m-1,A(m,n-1))$.

这又是一个递归定义，因为在(b)和(c)中，定义参照其自身. 注意到仅当 $m=0$ 时，$A(m,n)$才是明确给定的. 其基准为下述有序偶

$$(0,0),(0,1),(0,2),(0,3),\cdots,(0,n),\cdots.$$

尽管不能从定义明显看出 $A(m,n)$的值，但是它最终必可以由上述一个或多个基准有序偶的函数值表述出来.

在问题 3.24 中，我们计算了 $A(1,3)$的值. 对于如此简单的情况，也需要进行 15 个步骤的计算. 一般地说，除了平凡的情况外，Ackermann 函数值的计算是十分繁杂的. 它的重要性来自于数理逻辑. 我们之所以在这里给出，主要是作为递归函数的另一类示例，它说明递归函数定义中的递归部分可以是复杂的.

3.7　基　数

两个集合 A 与 B 称为是*对等的*，或*具有同样多的元素*，或*具有相同的基数*，记作 $A\simeq B$，如果存在一一对应 $f:A\to B$. 集合 A 称为*有限的*，如果对于某正整数 n，A 与集合$\{1,2,\cdots,n\}$具有相同的基数. 如果一个集合不是有限的，就称之为*无限的*. 熟知的无限集的例子有自然数集 **N**，整数集 **Z**，有理数集 **Q** 和实数集 **R**.

现在引入"基数"概念. 我们将基数简单地看做一种分配给集合的符号，两个集合被分配相同的符号当且仅当它们具有相同的基数. 集合 A 的基数通常记作$|A|$，$n(A)$或 card(A). 本书使用$|A|$.

有限集的基数符号是自然的. 即空集$\varnothing$为 0，集合$\{1,2,\cdots,n\}$的基数为 n. 于是$|A|=n$ 当且仅当 A 与$\{1,2,\cdots,n\}$具有相同的基数，即 A 含有 n 个元素.

正整数集 **N** 的基数为$\aleph_0$(读作"aleph 0"). 这个记号由 Cantor 引入. 于是$|A|=\aleph_0$ 当且仅当 A 与 **N** 具有相同的基数.

例 3.9　(a) $|\{x,y,z\}|=3$，$|\{1,3,5,7,9\}|=5$.

(b) 设 $E=\{2,4,6,\cdots\}$为正偶数的集合. 由 $f(n)=2n$ 定义的函数 $f:\mathbf{N}\to E$ 是正整数集合 **N** 与 E 之间的一个一一对应. 于是 E 与 **N** 有相同的基数，因此我们可以写

$$|E|=\aleph_0.$$

具有基数$\aleph_0$ 的集合称为*可数的*或*无限可数的*. 有限集和可数集都称为可数的. 可以证明有理数集 **Q** 是可数的. 下述定理(将在问题 3.15 中证明)以后将要用到.

定理 3.2　可数集的可数并仍然是可数的.

换句话说，如果 $A_1,A_2,\cdots$都是可数的，则并集

$$A_1\cup A_2\cup A_3\cup\cdots$$

也是可数集.

下面的定理给出了不可数无限集的一个重要的例子,该定理的证明见问题 3.16.

定理 3.3 从 0 到 1 的所有实数的集合 I 是不可数的.

基数与不等式

我们希望比较两个集合的大小.这由下面定义的基数之间的不等式关系给出.对于任意集合 A 与 B,定义 $|A|\leqslant|B|$,如果存在一一对应函数 $f: A\to B$.同样地,

$$|A|<|B| \quad 若 \quad |A|\leqslant|B| \quad 但 \quad |A|\neq|B|.$$

例如,因为由 $(n)=1/n$ 定义的函数 $f:\mathbf{N}\to I$ 是一一对应,但是由定理 3.3,$\mathbf{N}\neq|I|$,所以 $|\mathbf{N}|<|I|$.

在问题 3.28 中将证明的 Cantor 定理告诉我们,基数是无界的.

定理 3.4(Cantor) 对于任意集合 A,我们有 $|A|<|\text{Power}(A)|$(其中 Power(A) 为 A 的幂集,即 A 的全体子集族).

下面定理告诉我们,基数的不等式关系是对称的.

定理 3.5(Schroeder-Bernstein) 设集合 A 与 B 满足

$$|A|\leqslant|B| \quad 且 \quad |B|\leqslant|A|$$

则 $|A|=|B|$.

这个定理的等价形式将在问题 3.29 中证明.

3.8 算法与函数

算法 M 是求解一个特定问题的有限个良好定义的相继步骤的列表.比如,对于给定的函数 f 和输入值 X,求出 $f(X)$(其中 X 可以是一列值或值的集合).如下例所示,通常可以有不止一种方法求 $f(X)$.获得 $f(X)$ 的算法 M 的选择依赖于算法的"效率"和"复杂性",关于算法 M 的复杂性问题将在下一节讨论.

例 3.10 (多项式的值) 对于一个给定的多项式 $f(x)$ 和值 $x=a$,求 $f(a)$.比如已知

$$f(x)=2x^3-7x^2+4x-15, \quad 及 \quad a=5,$$

求 $f(a)$.这个问题可以由下列两种方法得到.

(a)(**直接法**) 将 $a=5$ 直接代入多项式进行计算

$$f(5)=2(125)-7(25)+4(5)-7=250-175+20-15=80.$$

我们共进行了 $4+3+1=8$ 次乘法和 3 次加法运算.一般地,用直接法求一个 n 次多项式的值大约需要

$$n+(n-1)+\cdots+1=\frac{n(n-1)}{2} \text{ 次乘法} \qquad 和 \qquad n \text{ 次加法}.$$

(b)(**Horner 方法或综合除法**) 我们利用逐步提取因子 x 的方法将多项式重新整理如下

$$f(x)=(2x^2-7x+4)x-15=((2x-7)x+4)x-15.$$

则

$$f(5)=((3)5+4)5-15=(19)5-15=95-15=80.$$

对于熟悉综合除法者,上述算法等价于下面的综合除法

$$\begin{array}{r|rrrrrrr} 5 & 2 & - & 7 & + & 4 & - & 15 \\ & & & 10 & + & 15 & + & 95 \\ \hline & 2 & + & 3 & + & 19 & + & 80 \end{array}$$

不难看出,上述用了 3 次乘法和 3 次加法.一般地,利用综合除法求一个 n 次多项式的值

大约需要

n 次乘法　和　n 次加法.

显然,综合除法(b)比直接法(a)有更高的效率.

例 3.11　(最大公约数)　设 a 与 b 为正整数,假定 $b<a$,求 a 与 b 的最大公约数 $d=\mathrm{GCD}(a,b)$. 解决这个问题有下面两种方法.

(a)(**直接法**)　先求出 a 与 b 的所有因子,比如对于 a,可以遍试从 2 到 $a/2$ 的所有数. 然后,取出它们的最大公因子. 例如,设 $a=258,b=60$. 求 a 与 b 的因子如下

$$a=258,\quad 因子:\quad 1,2,3,6,86,129,258$$

$$b=60,\quad 因子:\quad 1,2,3,4,5,6,10,12,15,20,30,60$$

从而,$d=\mathrm{GCD}(258,60)=6$.

(b)(**带余除法**)　首先以 b 除 a 得余数 r(注意 $r_1<b$). 然后以 r_1 除 b 得第二个余数 r_2(注意 $r_2<r_1$). 再以 r_2 除 r_1 得第三个余数 r_3(注意 $r_3<r_2$). 如此继续,以 r_{k-1} 除 r_k 得余数 r_{k+2}. 因为

$$a>b>r_1>r_2>r_3>\cdots. \qquad (*)$$

最终可以得到余数 $r_m=0$. 则 $r_{m-1}=\mathrm{GCD}(a,b)$. 例如,$a=258$, $b=60$. 则

(1) 以 $b=60$ 除 $a=258$ 得余数 $r_1=18$.

(2) 以 $r_1=18$ 除 $b=60$ 得余数 $r_2=6$.

(3) 以 $r_2=6$ 除 $r_1=18$ 得余数 $r_3=0$.

于是,$r_2=6=\mathrm{GCD}(258,60)$.

带余除法是求两个正整数 a,b 的最大公约数的非常有效的方法. 事实上,该算法由(*)决定,该算法得到 $d=\mathrm{GCD}(a,b)$ 并不是显然的,我们将在 11.6 中对此进行讨论.

3.9　算法的复杂性

算法分析是计算机科学的一项主要工作. 为了进行算法比较,我们必须给出算法效率的某种衡量标准. 本节就这个重要论题进行讨论.

假设 M 是一种算法,并设 n 为输入数据的规模. 实施 M 所占用的时间和空间是衡量该算法之效率的两个主要指标. 时间由"键盘操作"次数衡量. 比如

(a) 对于排序和查找,我们对比较次数计数.

(b) 在计算中,我们对乘法次数计数而忽略加法.

键盘操作的定义前提是其他操作时间大大小于或至多与键盘操作时间成比例. 空间由实施该算法所需的最大内存来衡量.

算法 M 的复杂性是一个函数 $f(n)$,它对于输入数据的规模 n 给出运行该算法所需时间与所需存储空间. 执行一个算法所需存储空间通常就是数据规模的倍数. 因此,除非特殊情况,"复杂性"将指运行算法的时间.

对于假定是指运行算法所需时间的复杂性函数 $f(n)$,它通常不仅仅与输入数据的规模有关,还与特定的数据有关. 例如,如果我们的任务是在一篇英文短故事 TEXT 中查找第一次出现的 3 个字母的单词 W. 显然,如果 W 为定冠词"the",则 W 有可能在 TEXT 的开头部分出现,于是 $f(n)$将会比较小. 另一方面,如果 W 是单词"zoo",则 W 甚至可能不会在 TEXT 中出现,所以 $f(n)$可能会很大.

上述讨论促使我们考虑对于适当的情况,求出复杂性函数 $f(n)$. 在复杂性理论中研究得最多的两种情况是:

(1) 最坏情况　对于任何可能的输入,$f(n)$的最大值.

(2) 平均情况　$f(n)$的期望值.

平均情况分析对于输入数据假定一个适当的概率分布,一种可取的假定是一个数据集合

的可能排列看上去是均等的. 平均情况还使用概率论中的下列概念. 假定数字 $n_1, n_2, \cdots, n_k$ 出现的概率分别为 $p_1, p_2, \cdots, p_k$. 则期望或均值 E 由下式给出:

$$E = n_1p_1 + n_2p_2 + \cdots + n_kp_k.$$

以下我们来建立这些概念.

线性查找

设给定了一个包含 n 个元素的线性数组 DATA, 和一个特定的信息 ITEM. 我们的任务是在数组 DATA 中求出 ITEM 的位置 LOC, 或者传送某个信息, 比如 LOC=0, 表示 ITEM 不出现于 DATA 中. 线性查找算法解决这个问题的途径是将 ITEM 与 DATA 中的元素一个一个地进行比较. 先将 ITEM 与 DATA[1]比较, 再与 DATA[2]比较, 如此继续, 直到 ITEM=DATA[LOC], 求出 LOC 为止.

线性查找算法的复杂性由 ITEM 与 DATA[K]之间的比较数字 C 给出. 我们来求 $C(n)$ 的最坏情况和平均情况.

(1) **最坏情况** 显然, 最坏情况是 ITEM 为数据组 DATA 的最后一个数据或根本就不在该数据组中. 在这两种情况下, 均有

$$C(n) = n.$$

于是, $C(n)=n$ 是线性查找算法的最坏情况.

(2) **平均情况** 这里我们假定 ITEM 在 DATA 中确实出现, 并且在数据组的任何位置出现概率均等. 因此, 比较次数可能是 $1, 2, 3, \cdots, n$ 中的任一个数, 而且每一个数出现的概率为 $1/p$. 则

$$\begin{aligned} C(n) &= 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n} \\ &= (1+2+\cdots+n) \cdot \frac{1}{n} \\ &= \frac{n(n+1)}{2} \cdot \frac{1}{n} \\ &= \frac{n+1}{2}. \end{aligned}$$

求出 ITEM 的位置所需比较的平均次数近似地等于数据组 DATA 中的数据个数的一半, 这个结果与我们的直觉是一致的.

注 一个算法的平均情况的复杂性的计算往往比最坏情况的复杂性的计算要繁杂得多. 而且, 对于平均情况中概率分布的一种假定常常在实际场合失效. 因此, 除非特别说明, 算法的复杂性将指对于给定输入数据的最坏情况确定运行时间的函数. 这个假设条件并不太强, 因为对于很多算法, 其平均情况的复杂性常与最坏情况的复杂性成比例.

增长率与大 O 记号

假定 M 是一个算法, 并设 n 为输入数据的大小. 显然 M 的复杂性 $f(n)$ 随着 n 的增大而增大. 通常我们需要考察的是 $f(n)$ 的增长率. 这常常由 $f(n)$ 与某标准函数相比较而得, 例如

$$\log_2 n, \quad n, \quad n\log_2 n, \quad n^2, \quad n^3, \quad 2^n,$$

等等, 都可被用作为标准函数. 这些标准函数的增长率如图 3-6 所示. 该图对于某些 n 的值给出了这些函数的对应近似值. 注意到这些函数是按其增长率列出的: 对数函数 $\log_2 n$ 增长最慢, 指数函数 2^n 增长最快, 而多项式函数 n^c 的增长率随其指数 c 的增大而变快.

$g(n)$ \ n	$\log n$	n	$n\log n$	n^2	n^3	2^n
5	3	5	15	25	125	32
10	4	10	40	100	10^3	10^3
100	7	100	700	10^4	10^6	10^{30}
1000	10	10^3	10^4	10^6	10^9	10^{300}

图 3－6　标准函数的增长率

将复杂性函数与一个标准函数相比较的一种方法是利用"大 O"记号，我们给出它的定义如下：

定义　设 $f(x)$与 $g(x)$为定义于 **R** 或 **R** 的子集上的任意两个函数. 我们说"$f(x)$与 $g(x)$同阶"，记作

$$f(x)=O(g(x)).$$

如果存在实数 k 和正常数 C 使得对于所有的 $x>k$ 有

$$|f(x)|\leqslant C|g(x)|.$$

同样地，当 $f(x)-h(x)=O(g(x))$时，记

$$f(x)=h(x)+O(g(x)).$$

（称上述为"大 O"是因为 $f(x)=o(g(x))$具有与其完全不同的意义.）

现考虑 m 次多项式 $P(x)$. 我们将在问题 3.27 中证明 $P(x)=O(x^m)$. 例如，由此有

$$7x^2-9x+4=O(x^2),\quad 及\quad 8x^3-576x^2+832x-248=O(x^3).$$

一些著名算法的复杂性

假设 $f(n)$与 $g(n)$为定义于正整数集上的函数. 则

$$f(n)=O(g(n))$$

意指对于所有的 n，$f(n)$以 $g(n)$的某常数倍为界.

为说明这种记号的方便之处，我们给出计算机科学中一些著名的查找和排序算法的复杂性.

(a) 线性查找：$O(n)$.
(b) 二叉查找：$O(\log n)$.
(c) 冒泡排序：$O(n^2)$.
(d) 归并排序：$O(n\log n)$.

问题与解答

函数

3.1　判断图 3－7 中的各图形是否定义了从 $A=\{a,b,c\}$到 $B=\{x,y,z\}$的函数.

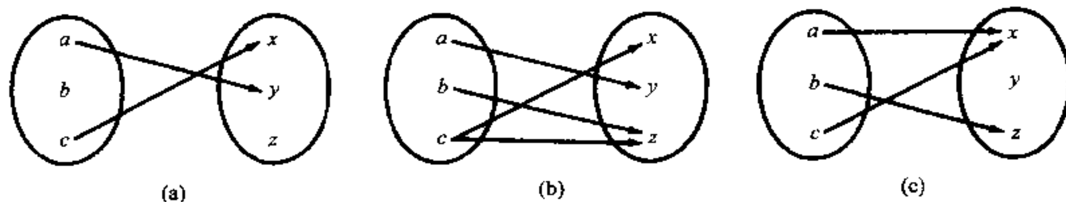


图 3－7

解 ☞　(a) 否. 因为没有对 $b\in A$ 分配对应值.

(b) 否. 对 $c\in A$ 分配了两个不同的元素 x 和 z.

(c) 是.

3.2 设 $X=\{1,2,3,4\}$. 试判定下列关系是否为 X 到 X 的函数.

(a) $f=\{(2,3),(1,4),(2,1),(3,2),(4,4)\}$.

(b) $g=\{(3,1),(4,2),(1,1)\}$.

(c) $h=\{(2,1),(3,4),(1,4),(2,1),(4,4)\}$.

解 ☞ 回忆 $X\times X$ 的一个子集 f 是函数 $f: X\to X$ 当且仅当对每一个 $a\in X$，它作为 f 的有序偶的第一分量出现恰好一次.

(a) 否. 2 作为 f 的两个相异有序偶(2,3)和(2,1)的第一分量.

(b) 否. 元素 $2\in X$ 没有作为 g 的有序偶的第一分量出现.

(c) 是. 尽管 $2\in X$ 作为第一元素出现于 h 的两个有序偶中，但这两个有序偶是相等的.

3.3 设 A 为某学校学生的集合. 试判断下列分配方法是否定义了 A 上的一个函数.

(a) 每个学生对应于其年龄.　　　　(b) 每个学生对应于其老师.

(c) 每个学生对应于其性别.　　　　(d) 每个学生对应于其配偶.

解 ☞ 对 A 的元素的一个分配能够成为 A 上的函数当且仅当 A 的每一个元素 a 恰被分配一个元素. 于是

(a) 是. 因为每个学生有且仅有一个年龄.

(b) 是，如果每个学生只有一位老师；否，如果有的学生有不止一个老师.

(c) 是.

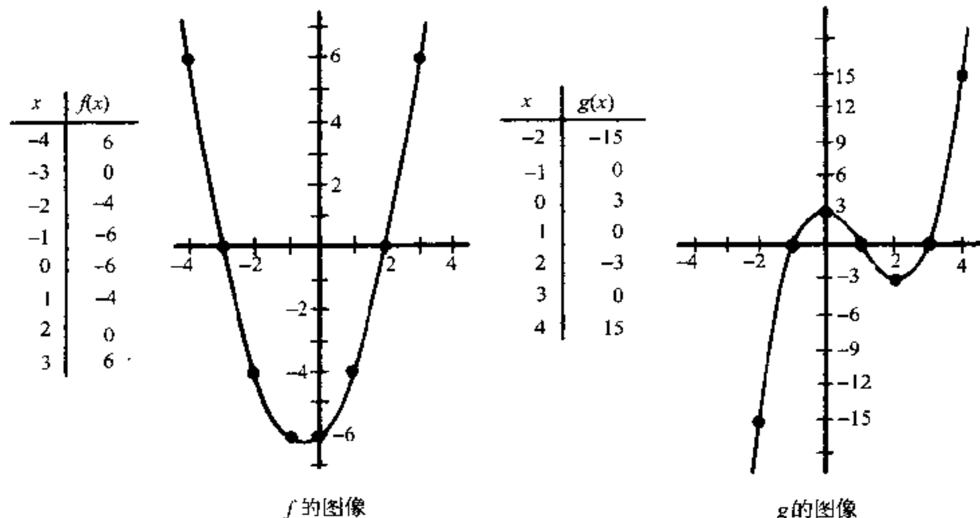
(d) 否，如果有学生未婚；是，如果每个学生都是已婚的.

3.4 画出下列函数的图形.

(a) $f(x)=x^2+x-6$.

(b) $g(x)=x^3-3x^2-x+3$.

解 ☞ 作出 x 与其对应函数值的表格. 因为所给函数为多项式函数，我们可以在坐标系中作出这些对应点，然后以光滑曲线将它们连起来，如图 3-8.



x	$f(x)$
−4	6
−3	0
−2	−4
−1	−6
0	−6
1	−4
2	0
3	6

x	$g(x)$
−2	−15
−1	0
0	3
1	0
2	−3
3	0
4	15

图 3-8

3.5 设函数 $f: A\to B$ 与 $g: B\to C$ 由图 3-9 定义. 求复合函数 $g\circ f: A\to C$.

解 ☞ 我们利用复合函数的定义来计算

$$(g\circ f)(a)=g(f(a))=g(y)=t,$$
$$(g\circ f)(b)=g(f(b))=g(x)=s,$$
$$(g\circ f)(c)=g(f(c))=g(y)=t.$$

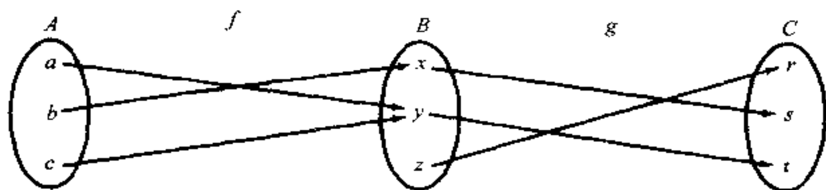


图 3-9

注意,如果我们"沿着图中的箭头"可以得到同样的结果

$$a \to y \to t,\quad b \to x \to s,\quad c \to y \to t.$$

3.6 设函数 f 与 g 的定义为 $f(x)=2x+1$ 与 $g(x)=x^2-2$. 求复合函数 $g\circ f$ 的表达式.

解 计算 $g\circ f$ 如下

$$(g\circ f(x)) = g(f(x)) = g(2x+1) = (2x+1)^2 - 2 = 4x^2+4x-1.$$

注意,这个问题同样可以按下面的方法来求解,令

$$y = f(x) = 2x+1,\quad z = g(y) = y^2-2.$$

从上式子中消去 y,得

$$z = y^2-2 = (2x+1)^2-2 = 4x^2+4x-1.$$

一一的,映上的和可逆函数

3.7 试判定下列函数是否为一一的.

(a) 对于地球上每一个人分配一个数字为其年龄.

(b) 对于世界上的每一个国家分配其首都的经度和纬度.

(c) 对于单一个署名作者的每一本书分配其作者.

(d) 对于世界上每一个设有总理的国家分配其总理.

解 (a) 否. 地球上可以有许多人具有相同的年龄.

(b) 是.

(c) 否. 因为一个作者可以写有不同的书.

(d) 是. 世界上的不同国家当然有不同的总理.

3.8 设函数 $f: A\to B$, $g: B\to C$, $h: C\to D$ 由图 3-10 定义.

(a) 判定是否每个函数都是映上的.

(b) 求复合函数 $h\circ g\circ f$.

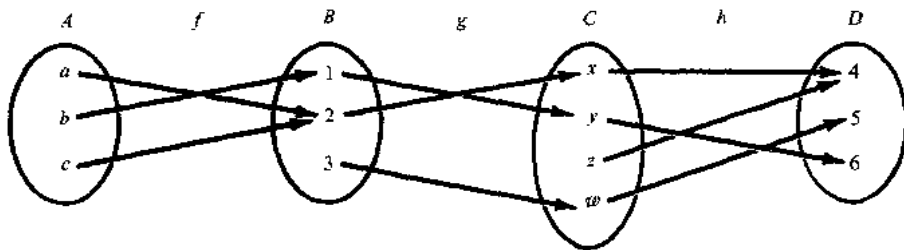


图 3-10

解 (a) 函数 $f: A\to B$ 不是映上的,因为 $3\in B$ 不是 A 中任何元素的像.

函数 $g: B\to C$ 不是映上的,因为 $z\in C$ 不是 B 中任何元素的像.

函数 $h: C\to D$ 是映上的,因为 D 的每一个元素都是 C 的某个元素的像.

(b) 因为 $a\to 2\to x\to 4$, $b\to 1\to y\to 6$, $c\to 2\to x\to 4$. 所以 $h\circ g\circ f=\{(a,4),(b,6),(c,4)\}$.

3.9 设函数 $f: A\to B$ 与 $g: B\to C$. 证明:

(a) 如果 f 与 g 都是一一的,则复合函数 $g\circ f$ 也是一一的.

(b) 如果 f 与 g 都是映上的，则 $g\circ f$ 也是映上的.

证明　(a) 设 $(g\circ f)(x)=(g\circ f)(y)$. 则 $g(f(x))=g(f(y))$. 因 g 是一一的，故 $f(x)=f(y)$. 进而，由 f 是一一的，有 $x=y$. 综上 $g\circ f$ 是一一的.

(b) 设 c 为 C 的任意元素. 因为 g 是映上的，故存在 $b\in B$ 使得 $g(b)=c$. 因为 f 是映上的，存在 $a\in A$ 使得 $f(a)=b$，然后

$$(g\circ f)(a)=g(f(a))=g(b)=c.$$

因此，对于这个任意的 $c\in C$，存在 $a\in A$ 以 c 为像，从而 $g\circ f$ 为映上的.

3.10　设 $f:\mathbf{R}\to\mathbf{R}$ 定义为 $f(x)=2x-3$. 则 f 为一一的，映上的，因此 f 可逆. 试求 f^{-1} 的表达式.

解答　设 y 为 x 在 f 下的像. 即

$$y=f(x)=2x-3.$$

则 x 应为 y 在 f^{-1} 下的像. 在方程中解出 x，得

$$x=(y+3)/2.$$

则 $f^{-1}(y)=(y+3)/2$. 以 x 代替 y，得

$$f^{-1}(x)=\frac{x+3}{2}.$$

这就是通常以 x 作为自变量的 f^{-1} 的表达式.

3.11　证明 De Morgan 律的推广：对于任意集类 $\{A_i\}$，有

$$(\bigcup_i A_i)^c=\bigcap_i A_i^c.$$

证明　我们有

$$x\in(\bigcup_i A_i)^c\Leftrightarrow x\notin\bigcup_i A_i\Leftrightarrow\forall i\in I, x\notin A_i\Leftrightarrow\forall i\in I, x\in A_i^c\Leftrightarrow x\in\bigcap_i A_i^c.$$

从而 $(\bigcup_i A_i)^c=\bigcap_i A_i^c$.（这里我们使用了逻辑记号 $\Leftrightarrow$ 表示"当且仅当"，$\forall$ 表示"对所有的"）.

基数

3.12　求下列集合的基数.

(a) $A=\{a,b,c,\cdots,y,z\}$.

(b) $B=\{1,-3,5,11,-28\}$.

(c) $C=\{x:x\in\mathbf{N},x^2=5\}$.

(d) $D=\{10,20,30,40,\cdots\}$.

(e) $E=\{6,7,8,9,\cdots\}$.

解答　(a) $|A|=26$. 因为共有 26 个英文字母.

(b) $|B|=5$.

(c) $|C|=0$. 因为不存在平方等于 5 的正整数，所以 C 为空集.

(d) $|D|=\aleph_0$. 因为由 $f(n)=10n$ 定义的函数 $f:\mathbf{N}\to D$ 为 $\mathbf{N}$ 与 D 之间的一一对应.

(e) $|E|=\aleph_0$. 因为由 $f(n)=n+5$ 定义的函数 $f:\mathbf{N}\to E$ 为 $\mathbf{N}$ 与 E 之间的一一对应.

3.13　证明整数集合 $\mathbf{Z}$ 的基数为 $\aleph_0$.

证明　下列图形表示了 $\mathbf{N}$ 与 $\mathbf{Z}$ 之间的一个一一对应.

$$\begin{array}{ccccccccccc}\mathbf{N} & = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots\\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots\\ \mathbf{Z} & = & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \cdots\end{array}$$

即下列函数 $f:\mathbf{N}\to\mathbf{Z}$ 是一一的和映上的

$$f(n)=\begin{cases}n/2, & n\text{ 为偶数},\\ (1-n)/2, & n\text{ 为奇数}.\end{cases}$$

于是，$|\mathbf{Z}|=|\mathbf{N}|=\aleph_0$.

3.14　设 $A_1,A_2,\cdots$ 为可数个有限集. 证明并集 $S=\bigcup_i A_i$ 也是可数的.

证明　我们首先列出 A_1 的元素，然后列出 A_2 的不属于 A_1 的元素，再列出 A_3 的不属于 A_1 或 A_2

(即前面没有列出过)的元素，如此继续下去. 因为 A_i 是有限集，我们总可以这样列出每一个集合的元素. 这个过程可以正式描述如下.

首先定义集合 $B_1, B_2, \cdots$，其中 B_i 包含 A_i 的不属于前面集合的元素，即定义

$$B_1 = A_1 \quad 和 \quad B_k = A_k \backslash (A_1 \cup A_2 \cup \cdots \cup A_{k-1}).$$

则 B_i 为不交的，且 $S = \bigcup_i B_i$. 设 $b_{i1}, b_{i2}, \cdots, b_{im_i}$ 为 B_i 的元素. 则 $S = \{b_{ij}\}$. 设 $f: S \to \mathbf{N}$ 定义为

$$f(b_{ij}) = m_1 + m_2 + \cdots + m_{i-1} + j.$$

如果 S 是有限的，则 S 是可数的. 如果 S 是无限的，则因为 f 是 S 与 $\mathbf{N}$ 之间的一一对应，S 是可数的.

3.15 证明定理 3.2：可数个可数集的并集是可数集.

证 ☞ 设 $A_1, A_2, A_3, \cdots$ 为可数个可数集. 特别地，假设 A_i 的元素为 $a_{i1}, a_{i2}, a_{i3}, \cdots$. 定义集合 $B_2, B_3, B_4, \cdots$ 如下

$$B_k = \{a_{ij} : i + j = k\}.$$

例如，$B_6 = \{a_{15}, a_{24}, a_{33}, a_{42}, a_{51}\}$. 注意到每个 B_k 都是有限集，且

$$S = \bigcup_i A_i = \bigcup_k B_k.$$

由上一题 $\bigcup_k B_k$ 是可数的，这里的 $S = \bigcup_i A_i$ 也是可数的. 定理得证.

3.16 证明定理 3.3：从 0 到 1 之间的实数的集合 I 是不可数的.

证 ☞ 因为 I 包含 $1, \frac{1}{2}, \frac{1}{3} \cdots$，故显然是一个无限集. 假设 I 是可数的. 则存在一一对应 $f: \mathbf{N} \to I$. 设 $f(1) = a_1, f(2) = a_2, \cdots$，即 $I = \{a_1, a_2, a_3, \cdots\}$. 我们用小数表示这些元素 $a_1, a_2, \cdots$ 并将其排成一列

$$a_1 = 0.x_{11}x_{12}x_{13}x_{14}\cdots,$$
$$a_2 = 0.x_{21}x_{22}x_{23}x_{24}\cdots,$$
$$a_3 = 0.x_{31}x_{32}x_{33}x_{34}\cdots,$$
$$a_4 = 0.x_{41}x_{42}x_{43}x_{44}\cdots,$$
$$\vdots$$

其中 $x_{ij} \in \{0, 1, 2, \cdots, 9\}$. (如果某数有两个不同的小数表达式，如 0.200 000 00⋯=0.199 999 9⋯，我们取以 9 结尾的一个.)

设 $b = 0.y_1y_2y_3y_4\cdots$ 为由下列方式得到的实数

$$y_i = \begin{cases} 1, & x_{ii} \neq 1, \\ 2, & x_{ii} = 1, \end{cases}$$

则 $b \in I$. 但

$$b \neq a_1 \quad 因 \quad y_1 \neq x_{11},$$
$$b \neq a_2 \quad 因 \quad y_2 \neq x_{22},$$
$$b \neq a_3 \quad 因 \quad y_3 \neq x_{33},$$
$$\vdots$$

于是 b 不属于 $I = \{a_1, a_2, \cdots\}$. 这与 $b \in I$ 矛盾. 因此关于 I 是可数的假设是错误的，故 I 不是可数的.

特殊数学函数

3.17 求(a) $\lfloor 7.5 \rfloor$；$\lfloor -7.5 \rfloor$；$\lfloor -18 \rfloor$；　(b) $\lceil 7.5 \rceil$；$\lceil -7.5 \rceil$；$\lceil -18 \rceil$.

解 ☞ (a) 由定义 $\lfloor x \rfloor$ 为不超过 x 的最大整数. 所以 $\lfloor 7.5 \rfloor = 7$，$\lfloor -7.5 \rfloor = -8$，$\lfloor -18 \rfloor = -18$.

(b) 由定义，$\lceil x \rceil$ 表示不小于 x 的最小整数. 所以 $\lceil 7.5 \rceil = 8$，$\lceil -7.5 \rceil = -7$，$\lceil -18 \rceil = -18$.

3.18 求(a) 25(mod 7)；(b) 25(mod 5)；(c) −35(mod 11)；(d) −3(mod 8).

解 ☞ 当 k 为正数时，直接以模数 M 除 k 得余数 r. 则 $r = k(\mathrm{mod}\ M)$. 当 k 为负时，以模数 M 除 $|k|$ 得余数 r'，则 $k(\mathrm{mod}\ M) = M - r'$(当 $r' \neq 0$). 于是

(a) 25(mod 7)=4，　(b) 25(mod 5)=0，

(c) −35(mod 11)=11−2=9，　(d) −3(mod 8)=8−3=5.

3.19 利用模 $M = 15$ 计算：

(a) 9+13；　(b) 7−11；　(c) 4−9；　(d) 2−10.

解☞ 利用 $a+M\equiv a(\bmod M)$：

(a) $9+13=22\equiv 22-15=7$. (b) $7+11=18\equiv 18-15=3$.

(c) $4-9=-5\equiv -5+15=10$. (d) $2-10=-8\equiv -8+15=7$.

3.20 化简： (a) $\dfrac{n!}{(n-1)!}$； (b) $\dfrac{(n+2)!}{n!}$.

解☞ (a)

$$\frac{n!}{(n-1)!}=\frac{n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}=n,$$

或简单地，

$$\frac{n!}{(n-1)!}=\frac{n(n-1)!}{(n-1)!}=n.$$

(b)

$$\begin{aligned}\frac{(n+2)!}{n!}&=\frac{(n+2)(n+1)n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}\\&=(n+2)(n+1)=n^2+3n+2,\end{aligned}$$

或简单地，

$$\frac{(n+2)!}{n!}=\frac{(n+2)(n+1)n!}{n!}=(n+2)(n+1)=n^2+3n+2.$$

3.21 求值： (a) $\log_2 8$； (b) $\log_2 64$； (c) $\log_{10} 100$； (d) $\log_{10} 0.001$.

解☞ (a) $\log_2 8=3$，因为 $2^3=8$.

(b) $\log_2 64=6$，因为 $2^6=64$.

(c) $\log_{10}100=2$，因为 $10^2=100$.

(d) $\log_{10}0.001=-3$，因为 $10^{-3}=0.001$.

注 对数通常用近似值给出. 比如，利用对数表或计算器，可得下列对数的近似值(其中 $e=2.718281\cdots$)

$$\log_{10}300=2.4771,\quad \log_e 40=3.6889$$

递归函数

3.22 设 a 与 b 为正整数，并设 Q 的递归定义如下

$$Q(a,b)=\begin{cases}0, & a<b,\\ Q(a-b,b)+1, & b\leqslant a.\end{cases}$$

(a) 求：(i) $Q(2,5)$，(ii) $Q(12,5)$.

(b) 函数 Q 的实际意义是什么？求 $Q(5861,7)$.

解☞ (a) (i) $Q(2,5)=0$，因为 $2<5$.

(ii)
$$\begin{aligned}Q(12,5)&=Q(7,5)+1\\&=[Q(2,5)+1]+1\\&=Q(2,5)+2\\&=0+2=2.\end{aligned}$$

(b) 每次从 a 减去 b，Q 的值增加 1. 因此 $Q(a,b)$ 给出了 a 除以 b 的商. 于是 $Q(5861,7)=837$.

3.23 设 n 为正整数. 函数 L 的递归定义如下

$$L(n)=\begin{cases}0, & n=1,\\ L(\lfloor n/2\rfloor)+1, & n>1.\end{cases}$$

求 $L(25)$ 并对这个函数进行描述.

解☞ 求 $L(25)$ 的递归过程如下

$$\begin{aligned}L(25)&=L(12)+1\\&=[L(6)+1]+1\\&=L(6)+2\end{aligned}$$

$$
\begin{aligned}
&= [L(3)+1]+2\\
&= L(3)+3\\
&= [L(1)+1]+3\\
&= L(1)+4\\
&= 0+4 = 4.
\end{aligned}
$$

每当 n 除以 2 时，L 就增加 1. 因此 L 是满足

$$2^l \leqslant n$$

的最大整数. 由此，

$$L(n) = \lfloor \log_2 n \rfloor.$$

3.24 利用 Ackermann 函数的定义求 $A(1,3)$.

解 我们需要进行如下的 15 步运算：

(1) $A(1,3)=A(0,A(1,2))$
(2) $A(1,2)=A(0,A(1,1))$
(3) $A(1,1)=A(0,A(1,0))$
(4) $A(1,0)=A(0,1)$
(5) $A(0,1)=1+1=2$
(6) $A(1,0)=2$
(7) $A(1,1)=A(0,2)$
(8) $A(0,2)=2+1=3$
(9) $A(1,1)=3$
(10) $A(1,2)=A(0,3)$
(11) $A(0,3)=3+1=4$
(12) $A(1,2)=4$
(13) $A(1,3)=A(0,4)$
(14) $A(0,4)=4+1=5$
(15) $A(1,3)=5$.

排在靠前位置的式子表示我们在提取定义并推迟确定函数值，而排在靠后位置的式子则表示回代计算. 注意到，函数的定义在(a) 5,8,11,14 步；(b) 第 4 步和(c)第 1,2,3 步中被使用. 其他步骤是进行回代计算.

杂题

3.25 对于下列每个实变量的实值函数，求其定义域 D.

(a) $f(x)=\dfrac{1}{x-2}$.　　(b) $f(x)=x^2-3x-4$.

(c) $f(x)=\sqrt{25-x^2}$.　　(d) $f(x)=x^2, 0\leqslant x\leqslant 2$.

解 当一个实变量的实值函数由公式 $f(x)$ 给定时，除非有特别声明，其定义域 D 就是使得 $f(x)$ 有意义的 $\mathbf{R}$ 的最大子集.

(a) 当 $x-2=0$ 即 $x=2$ 时，f 无定义，因此 $D=\mathbf{R}\setminus\{2\}$.

(b) f 对任意实数有定义，所以 $D=\mathbf{R}$.

(c) 当 $25-x^2$ 为负数时，f 无定义，所以 $D=[-5,5]=\{x: -5\leqslant x\leqslant 5\}$.

(d) f 的定义域已由题目明确规定，即 $D=\{x: 0\leqslant x\leqslant 2\}$.

3.26 对于任意的 $n\in\mathbf{N}$，设 $D_n=(0,1/n)$ 表示从 0 到 $1/n$ 的开区间. 求：

(a) $D_3\cup D_7$；(b) $D_3\cap D_{20}$；(c) $D_s\cup D_t$；(d) $D_s\cap D_t$.

解 (a) 因为 $(0,1/3)$ 是 $(0,1/7)$ 的母集，所以 $D_3\cup D_7=D_3$.

(b) 因为 $(0,1/20)$ 是 $(0,1/3)$ 的一个子集，所以 $D_3\cap D_{20}=D_{20}$.

(c) 设 $m=\min(s,t)$，即为 s 与 t 两者中较小的一个. 则 D_m 等于 D_s 或 D_t 而包含余下的一个集合作为其子集. 因此，$D_s\cup D_t=D_m$.

(d) 设 $M=\max(s,t)$，即 s 与 t 中较大的一个. 则 $D_s\cap D_t=D_M$.

3.27 设 $P(n)=a_0+a_1n+a_2n^2+\cdots+a_mn^m$ 的次数为 m. 证明 $P(n)=O(n^m)$.

证 ☞ 设 $b_0=|a_0|, b_1=|a_1|, \cdots, b_m=|a_m|$. 则对于 $n\geqslant 1$,

$$\begin{aligned}P(n) &\leqslant b_0+b_1n+b_2n^2+\cdots+b_mn^m\\ &=\left(\frac{b_0}{n^m}+\frac{b_1}{n^{m-1}}+\cdots+b_m\right)n^m\\ &\leqslant (b_0+b_1+\cdots+b_m)n^m\\ &=Mn^m,\end{aligned}$$

其中 $M=|a_0|+|a_1|+\cdots+|a_m|$. 所以, $P(n)=O(n^m)$.

例如, $5x^3+3x=O(x^3)$ 及 $x^5-4000000x^2=O(x^5)$.

3.28 证明定理 3.4(Cantor): $|A|<|\mathrm{Power}(A)|$ (其中 $\mathrm{Power}(A)$ 为 A 的幂集).

证 ☞ 显然,由 $g(a)=\{a\}$ 定义的函数 $g: A\to\mathrm{Power}(A)$ 为一一对应,所以 $|A|\leqslant|\mathrm{Power}(A)|$. 为完成定理的证明,只要证明 $|A|\neq|\mathrm{Power}(A)|$. 反设 $|A|=|\mathrm{Power}(A)|$, 且 $f: A\to\mathrm{Power}(A)$ 为一一的映上的. 若 $a\notin f(a)$, 就设 a 为一个"坏"元素,并设 B 为所有坏元素的集合. 换言之,

$$B=\{x: x\in A, x\notin f(x)\}.$$

现在 B 是 A 的一个子集. 因为 $f: A\to\mathrm{Power}(A)$ 是映上的,存在 $b\in A$ 使得 $f(b)=B$. 那么 b 是"好"元素还是"坏"元素呢? 如果 $b\in B$, 则 $b\notin f(b)=B$ 这是不可能的. 同样,如果 $b\notin B$, 则 $b\in f(b)=B$, 这也是不可能的. 于是原假设 $|A|=|\mathrm{Power}(A)|$ 导致矛盾,故该假设错误,定理的结论成立.

3.29 证明 Schroeder-Bernstein 定理 3.5 的等价公式:设 $X\supseteq Y\supseteq X_1$ 以及 $X\simeq X_1$. 则 $X\simeq Y$.

证 ☞ 因为 $X\simeq X_1$, 所以存在一一对应(双射) $f: X\to X_1$. 因为 $X\supseteq Y$, 故 f 在 Y 上的限制也是一一对应,我们仍记之为 f. 设 $f(Y)=Y_1$. 则 Y 与 Y_1 为对等的,

$$X\supseteq Y\supseteq X_1\supseteq Y_1$$

且 $f: Y\to Y_1$ 为双射. 但我们有 $Y\supseteq X_1\supseteq Y_1$ 且 $Y\simeq Y_1$. 同理, X_1 与 $f(X_1)=X_2$ 对等,

$$X\supseteq Y\supseteq X_1\supseteq Y_1\supseteq X_2$$

且 $f: X_1\to X_2$ 为双射. 由此,存在对等的集合 $X, X_1, X_2, \cdots$ 与 $Y, Y_1, Y_2, \cdots$ 使得

$$X\supseteq Y\supseteq X_1\supseteq Y_1\supseteq X_2\supseteq Y_2\supseteq X_3\supseteq Y_3\supseteq\cdots$$

且 $f: X_k\to X_{k+1}$ 与 $f: Y_k\to Y_{k+1}$ 均为双射.

设

$$B=X\cap Y\cap X_1\cap Y_1\cap X_2\cap Y_2\cap\cdots,$$

则

$$X=(X\backslash Y)\cup(Y\backslash X_1)\cup(X_1\backslash Y_1)\cup\cdots\cup B,$$
$$Y=(Y\backslash X_1)\cup(X_1\backslash Y_1)\cup(Y_1\backslash X_2)\cup\cdots\cup B.$$

进而, $X\backslash Y, X_1\backslash Y_1, X_2\backslash Y_2, \cdots$ 为对等的. 事实上,函数

$$f: (X_k\backslash Y_k)\to(X_{k+1}\backslash Y_{k+1})$$

为一一的和映上的.

考虑函数 $g: X\to Y$ 由图 3-11 定义. 即

$$g(x)=\begin{cases}f(x), & x\in X_k\backslash Y_k \text{ 或 } x\in X\backslash Y,\\ x, & x\in Y_k\backslash X_k \text{ 或 } x\in B.\end{cases}$$

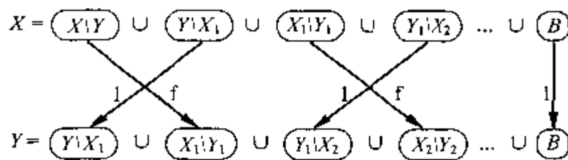


图 3-11

补 充 题

函数

3.30 设 $W=\{a,b,c,d\}$. 试判定下列有序偶的集合是否为 W 到 W 的函数.

(a) $\{(b,a),(c,d),(d,a),(c,d),(a,d)\}$.

(b) $\{(d,d),(c,a),(a,b),(d,b)\}$.

(c) $\{(a,b),(b,b),(c,b),(d,b)\}$.

(d) $\{(a,a),(b,a),(a,b),(c,d)\}$.

3.31 已知集合{Britt, Martin, Daivid, Alan, Rebecca}. 设函数 g 对集合中的每一个名字分配拼出该名字的字母数，请将 g 写为有序偶的集合.

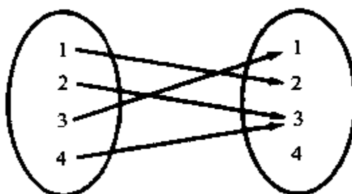


图 3－12

3.32 设 $W=\{1,2,3,4\}$并设 $g: W\to W$，如图 3－12 所定义.

(a) 将 g 写为有序偶的集合.

(b) 求 g 的像.

(c) 以有序偶的集合的形式写出复合函数 $g\circ g$.

3.33 设 $V=\{1,2,3,4\}$并设

$$f=\{(1,3),(2,1),(3,4),(4,3)\} \quad 及 \quad g=\{(1,2),(2,3),(3,1),(4,1)\}.$$

求：(a) $f\circ g$;　(b) $g\circ f$;　(c) $f\circ f$.

3.34 设 $f: \mathbf{R}\to\mathbf{R}$ 的定义为 $f(x)=3x-7$. 求 $f^{-1}: \mathbf{R}\to\mathbf{R}$ 的表达式.

函数的性质

3.35 证明：如果 $f: A\to B$ 与 $g: B\to A$ 满足 $g\circ f=1_A$，则 f 为一一的，g 为映上的.

3.36 证明定理 3.1：函数 $f: A\to B$ 是可逆的当且仅当 f 既是一一的也是映上的.

3.37 证明：若 $f: A\to B$ 是可逆的，且具有逆函数 $f^{-1}: B\to A$，则 $f^{-1}\circ f=1_A$ 且 $f\circ f^{-1}=1_B$.

3.38 对于 $\mathbf{N}$ 中的每个正整数 n，设 A_n 为实数集 $\mathbf{R}$ 的下列子集

$$A_n=(0,1/n)=\{x: 0<x<1/n\}.$$

求：

(a) $A_5\cup A_8$.　　(b) $A_3\cap A_7$.

(c) $\cup(A_i: i\in J)$.　　(d) $\cap(A_i: i\in J)$.

(e) $\cup(A_i: i\in K)$.　　(f) $\cap(A_i: i\in K)$.

其中 J 为 $\mathbf{N}$ 的有限子集，而 K 为 $\mathbf{N}$ 的无限子集.

3.39 考虑集合的指标类$\{A_i: i\in I\}$，B 为一个集合，i_0 为 I 的元素. 证明：

(a) $B\cap(\cup_i A_i)=\cup_i(B\cap A_i)$.

(b) $\cap(A_i: i\in I)\subseteq A_{i_0}\subseteq\cup(A_i: i\in I)$.

3.40 对于 $\mathbf{N}$ 中的每个正整数 n，设 D_n 为 $\mathbf{N}$ 的如下定义的子集

$$D_n=\{n,2n,3n,4n,\cdots\}=\{n 的倍数\}.$$

(a) 求：(1) $D_2\cap D_7$；(2) $D_6\cap D_8$；(3) $D_3\cup D_{12}$；(4) $D_3\cap D_{12}$.

(b) 证明 $\cap(D_i: i\in J)=\varnothing$，其中 J 为 $\mathbf{N}$ 的一个无限子集.

基数

3.41 求下列集合的基数.

(a) {星期一，星期二，…，星期天}.

(b) $\{x: x$ 是单词 BASEBALL 中的一个字母$\}$.

(c) $\{x: x^2=9, 2x=8\}$.

(d) 集合 $A=\{1,5,7,11\}$的幂集 Power(A).

(e) 从集合 $A=\{a,b,c\}$到集合 $B-\{1,2,3,4\}$的函数的集合.

(f) 集合 $A=\{a,b,c\}$上的关系的集合.

3.42 证明：

(a) 每个无限集 A 具有一个可数子集 D.

(b) 可数集的每个子集都是有限的或可数的.

(c) 若 A 与 B 均为可数的,则 $A\times B$ 也是可数的.

(d) 有理数集 $\mathbf{Q}$ 是可数的.

3.43 证明:

(a) $|A\times B|=|B\times A|$.

(b) 若 $A\subseteq B$,则 $|A|\leqslant|B|$.

(c) 若 $|A|=|B|$,则 $|P(A)|=|P(B)|$.

3.44 求下列集合的基数.

(a) 从集合 $A=\{a,b,c,d\}$ 到集合 $B=\{1,2,3,4,5\}$ 的函数的集合 X.

(b) 集合 $A=\{a,b,c,d\}$ 上所有关系的集合 Y.

特殊函数

3.45 求:

(a) $\lfloor 13.2\rfloor$,$\lfloor -0.17\rfloor$,$\lfloor 34\rfloor$.

(b) $\lceil 13.2\rceil$,$\lceil -0.17\rceil$,$\lceil 34\rceil$.

3.46 求:(a) $10(\bmod 3)$;(b) $200(\bmod 20)$;(c) $5(\bmod 12)$;(d) $29(\bmod 6)$;(e) $-347(\bmod 6)$;(f) $-555(\bmod 11)$.

3.47 求:(a) $3!+4!$;(b) $3!(3!+2!)$;(c) $6!/5!$;(d) $30!/28!$.

3.48 求值:(a) $\log_2 16$;(b) $\log_3 37$;(c) $\log_{10} 0.01$.

杂题

3.49 证明:所有整系数多项式

$$p(x)=a_0+a_1x+\cdots+a_mx^m$$

的集合为可数的,其中 $a_0,a_1,\cdots,a_m$ 为整数.

3.50 设 a,b 为整数,$Q(a,b)$ 的递归定义如下

$$Q(a,b)=\begin{cases}5, & a<b,\\ Q(a-b,b+2)+a, & a\geqslant b.\end{cases}$$

求:$Q(2,7)$,$Q(5,3)$,$Q(15,2)$.

补充题答案

3.30 (a) 是;(b) 否;(c) 是;(d) 否.

3.31 $g=\{$(britt,4),(Martin,6),(Daivid,4),(Alan,3),(Rebecca,5)$\}$.

3.32 (a) $g=\{(1,2),(2,3),(3,1),(4,3)\}$;

(b) $\{1,2,3\}$.

(c) $g\circ g=\{(1,3),(2,1),(3,2),(4,1)\}$.

3.33 (a) $\{(1,1),(2,4),(3,3),(4,3)\}$.

(b) $\{(1,1),(2,2),(3,1),(4,1)\}$.

(c) $\{(1,4),(2,3),(3,3),(4,4)\}$.

3.34 $f^{-1}=\dfrac{x+7}{3}$.

3.38 (a) A_5;(b) A_7;

(c) A_r,其中 r 是 J 中的最小整数;

(d) A_s,其中 s 是 J 中的最大整数;

(e) A_r,其中 r 是 K 中的最小整数;

(f) $\varnothing$.

3.40 (1) D_{14};(2) D_{24};(3) D_3;(4) D_{12}.

3.41 (a) 7;(b) 5;(c) 0;(d) 16;(e) $4^3=64$;(f) $2^9=512$.

3.44 (a) $5^4=625$; (b) $2^{16}=65,536$.

3.45 (a) $13,-1,34$; (b) $14,0,34$.

3.46 (a) 1; (b) 0; (c) 2; (d) 5; (e) $6-5=1$; (f) $11-5-6$.

3.47 (a) 30; (b) 48; (c) 6; (d) 870.

3.48 (a) 4; (b) 3; (c) -2.

3.49 提示:设 P_k 为所有满足 $m\leqslant k$ 且每个 $|a_i|\leqslant m$ 的多项式 $p(x)$ 的集合,则 P_k 为有限的且 $P=\bigcup_k P_k$.

3.50 $Q(2,7)=5$, $Q(5,3)=10$; $Q(15,2)=42$.

第四章　逻辑与命题演算

4.1 引　言

数学中的许多证明过程和计算机科学中的算法都采用诸如

"如果 p 则 q"　或者　"如果 p_1 且 p_2，则 q_1 或 q_2"

等逻辑表达式. 因为我们需要的是那些能够作为真值而参照的表述，所以对于这些表述是真或假的研究是非常必要的. 本章将讨论这些内容.

我们还将考察量词陈述的真值，哪些是陈述，哪些使用了逻辑量词"对每个"和"存在".

4.2 命题与复合命题

一个命题(或陈述)是一个说明性语句，它只能是真或是假，不可能两者同时成立. 例如，我们考虑下列八个语句：

(i) 巴黎在法国.

(ii) $1+1=2$.

(iii) $2+2=3$.

(iv) 伦敦在丹麦.

(v) $9<6$.

(vi) $x=2$ 是 $x^2=4$ 的一个解.

(vii) 你去哪儿?

(viii) 做你的作业.

除(vii)和(viii)外，其余都是命题. 但是其中(i)，(ii)，(vi)为真，(iii)，(iv)，(v)为假.

复合命题

许多命题是复合的，即由一些子命题及它们之间的各种联系组成. 这样的命题称为*复合命题*. 不能被分解为更简单的命题，即不是复合的命题称为*原子命题*.

例 4.1 (a) "玫瑰是红的而紫罗兰是蓝的"是一个复合命题，含有子命题"玫瑰是红的"和"紫罗兰是蓝的".

(b) "约翰很聪明或每天晚上学习"是一个复合命题，含有子命题"约翰很聪明"和"约翰每天晚上学习".

(c) 前述的命题(i)到(vi)都是原子命题，它们不能被分解为更简单的命题.

> 复合命题的基本性质是其真值可以由其子命题的真值以及它们复合成该复合命题的联结方式完全确定. 下节将研究这些联结.

4.3 基本逻辑运算

本节将讨论三个基本的逻辑运算：合取联结，析取联结和否定联结，分别对应于"与"，"或"，"非"三个术语.

合取联结，$p \wedge q$

任何两个命题可以用术语"与"联合而成一个复合命题，叫做这两个原始命题的合取联结，记作

$$p \wedge q.$$

读作“p 与 q”，表示 p 与 q 的合取联结. 因为 $p\wedge q$ 是一个命题，所以它具有其真值，这个真值仅与 p 与 q 的真值有关. 特别地，

定义 4.1　如果 p 与 q 均为真，则 $p\wedge q$ 为真；否则 $p\wedge q$ 为假.

命题 $p\wedge q$ 的真值可以用图 4－1(a)中的表来给出量化定义. 其中，第一行是如果 p 与 q 均为真，则 $p\wedge q$ 为真的一种简洁说法. 第二行说如果 p 真，q 假则 $p\wedge q$ 为假，等等. 考察该表可见，对于两个子命题 p 与 q 的 T 和 F 组合，表格中一共有四行对应于四种可能情况. 注意仅当 p 与 q 均为真时，才有 $p\wedge q$ 为真.

例 4.2　考虑下列四个陈述语句：

(i) 巴黎在法国与 2+2=4.

(ii) 巴黎在法国与 2+2=5.

(iii) 巴黎在英国与 2+2=4.

(iv) 巴黎在英国与 2+2=5.

只有第一个陈述语句为真. 其他陈述语句都为假，因为其中至少有一个子命题为假.

p	q	$p\wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

(a) “p 与 q”

p	q	$p\vee q$
T	T	T
T	F	T
F	T	T
F	F	F

(b) “p 或 q”

p	$\neg p$
T	F
F	T

(c) “非 p”

图 4－1

析取联结，$p\vee q$

任何两个命题可以用术语“或”联合而成一个复合命题，叫做这两个原始命题的析取联结，记作

$$p \vee q.$$

读作“p 或 q”，表示 p 与 q 的析取联结. $p\vee q$ 的真值仅与 p 与 q 的真值有关，如下列定义.

定义 4.2　如果 p 与 q 均为假，则 $p\vee q$ 为假；否则 $p\wedge q$ 为真.

命题 $p\vee q$ 的真值可以用图 4－1(b)中的表来给出量化定义. 注意 $p\vee q$ 为假仅出现于第四种情况，即当 p 与 q 均为假时.

例 4.3　考虑下列四个陈述语句：

(i) 巴黎在法国或 2+2=4.

(ii) 巴黎在法国或 2+2=5.

(iii) 巴黎在英国或 2+2=4.

(iv) 巴黎在英国或 2+2=5.

只有陈述语句(iv)为假. 其他陈述语句都为真，因为其中至少有一个子命题为真.

注　“或”通常会有两种不同的用途. 一种情况是用在如“p 或 q 或两者均可”的表述中，即两个选择中至少有一种出现，如上面讨论的. 另一种是使用在如“p 或 q 但不是两者均可”的表述中，即两种选择恰好有一种出现. 例如，在语句“他将要上哈佛或耶鲁”中使用的“或”，我们将后一种情况称为*排斥析取联结*. 除非有特别说明，我们仅用前一种意义下的“或”. 这里的讨论明确规定了符号语言 $p\vee q$ 的涵义，它由真值表定义，并且总是表示“p 与/或 q”.

否定联结，$\neg p$

给定任一个命题 p，都可以通过在 p 前面添加“不是”或“假”或如果可能的话在 p 前面插入“非”，得到另一个命题，称为 p 的*否定联结*，记作

$$\neg p,$$

读作“非 p”，表示 p 的否定联结. $\neg p$ 的真值按如下定义描述，与 p 的真值有关.

定义 4.3 如果 p 为真，则 $\neg p$ 为假；如果 p 为假，则 $\neg p$ 为真.

$\neg p$ 的真值可以量化定义如图 4－1(c)中的表. p 的否定联结的真值总是与 p 的真值相反.

例 4.4 考虑下列六个陈述语句：

(a_1) 巴黎在法国. (b_1) $2+2=5$.

(a_2) 巴黎在法国是不对的. (b_2) $2+2=5$ 是不对的.

(a_3) 巴黎不在法国. (b_3) $2+2\neq 5$.

(a_2)，(a_3)都是(a_1)的否定联结，(b_2)，(b_3)都是(b_1)的否定联结. 因为(a_1)为真，所以(a_2)，(a_3)都为假；同样地，因为(b_1)真，所以(b_2)，(b_3)都为假.

注 “与”，“或”，“非”的逻辑符号并不完全统一，比如有些教科书中使用下面的对应记号

$$p\&q, p\cdot q, pq, \quad p\wedge q.$$
$$p+q, \quad p\vee q.$$
$$p', \bar{p}, \sim p, \quad \neg p.$$

4.4 命题与真值表

设 $P(p,q,\cdots)$ 为一个由取值为真(T)或假(F)的逻辑变量 $p,q,\cdots$ 以及逻辑联结 $\wedge$；$\vee$；$\neg$（和今后将要讨论的其他逻辑联结）构成的表达式. 这样的表达式 $P(p,q,\cdots)$ 称为一个*命题*.

命题 $P(p,q,\cdots)$ 的主要性质是它的真值只与其逻辑变量的真值有关，即一旦每个逻辑变量的真值为已知，则命题的真值也就确定了. 说明这个关系的一个简洁方法是利用*真值表*. 下面我们给出获得真值表的一种方法.

例如，考虑命题 $\neg(p\wedge\neg q)$. $\neg(p\wedge\neg q)$ 的真值表的构造方法如图 4－2 所示. 注意到开始的列表示逻辑变量 $p,q,\cdots$，表格中应有足够多的行来列出这些变量所有可能的 T，F 组合.（对于 2 变量，需要 4 行；3 变量需要 8 行；一般地，对于 n 个变量，必须要有 2^n 行.）然后，对于构成命题的每一个“基本”步骤，表格中都对应有一列，每一步的真值都利用联结 $\wedge$，$\vee$，$\neg$ 的定义依据前面的步骤确定. 在表格的最后一列，我们获得命题的真值.

命题 $\neg(p\wedge\neg q)$ 的实际真值表如图 4－2(b)，它由图 4－2(a)中相对于变量和命题的列构成，而图 4－2(a)中的其他列的作用仅仅是为构造真值表做准备.

p	q	$\neg q$	$p\wedge\neg q$	$\neg(p\wedge\neg q)$
T	T	F	F	T
T	F	T	T	F
F	T	F	F	T
F	F	T	F	T

(a)

p	q	$\neg(p\wedge\neg q)$
T	T	T
T	F	F
F	T	T
F	F	T

(b)

图 4－2

注 为避免出现太多的括号，我们对逻辑联结规定优先级. 特别地，

$\neg$ 优先于 $\wedge$ 优先于 $\vee$

例如，$\neg p\wedge q$ 意指 $(\neg p)\vee q$ 而不是 $\neg(p\wedge q)$.

构造真值表的另一种方法

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T					
T	F					
F	T					
F	F					
步骤						

图 4－3

下面给出构造 $\neg(p\wedge\neg q)$ 真值表的另一种方法.

(a) 首先构造如图 4－3 所示的真值表. 即首先列出所有变量及其真值. 然后将命题写在变量右边的第一行，并使得命题中的每个变量和联结都占有一列的位置. 表格的最后一行标为“步骤”.

(b) 分步骤将真值填入真值表，如图 4－4 所示. 即首先将

变量的真值填入其在命题栏对应的列，然后，对每个逻辑运算都在其对应列填入真值. 也就是说，与步骤栏对应，每一步都在其对应列填上了真值.

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T		T			T
T	F		T			F
F	T		F			T
F	F		F			F
步骤			1			1

(a)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T		T		F	T
T	F		T		T	F
F	T		F		F	T
F	F		F		T	F
步骤			1		2	1

(b)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T		T	F	F	T
T	F		T	T	T	F
F	T		F	F	F	T
F	F		F	F	T	F
步骤			1	3	2	1

(c)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
T	T	T	T	F	F	T
F	T	F	T	T	T	F
F	F	T	F	F	F	T
F	F	T	F	F	T	F
步骤		4	1	3	2	1

(d)

图 4－4

于是，命题的真值表由变量的列和最后一步构成，最后一步是指最后填入真值的列.

4.5 永真命题和永假命题

有些命题 $P(p,q,\cdots)$ 在其真值表的最后一列只含有 T，换句话说，对于变量的任意真值它们都为真. 这样的命题称为*永真命题*. 类似地，一个命题 $P(p,q,\cdots)$ 称为*永假命题*，如果其真值表的最后一列只含有 F，换句话说，对于其变量的任意真值，命题都为假. 例如，命题"p 或非 p"即 $p\vee\neg p$ 为永真命题，而命题"p 与非 p"即 $p\wedge\neg p$ 为永假命题. 这在图 4－5 的真值表中再次得到验证.（因为每个命题只有一个变量 p，所以真值表只有两行.）

p	$\neg p$	$p\vee\neg p$
T	F	T
F	T	T

(a) $p\vee\neg p$

p	$\neg p$	$p\wedge\neg p$
T	F	F
F	T	F

(b) $p\wedge\neg p$

图 4－5

因为永假命题总是假的，而永真命题总是真的，所以永真命题的否定是永假命题，永假命题的否定是永真命题.

设 $P(p,q,\cdots)$ 是永真命题，而 $P_1(p,q,\cdots)$，$P_2(p,q,\cdots)$，…是任意命题. 因为 $P(p,q,\cdots)$ 与其变量的真值无关，我们可以在永真命题中以命题 P_1，P_1，…分别代替变量 p，q，…仍然得到一个永真命题. 换句话说：

定理 4.1（代入原理） 若 $P(p,q,\cdots)$ 是永真命题，则对任意命题 $P_1,P_2,\cdots$，命题 $P(P_1,P_2,\cdots)$ 仍然是永真命题.

4.6 逻辑等价

两个命题 $P(p,q,\cdots)$ 与 $Q(p,q,\cdots)$ 称为*逻辑等价的*，或简称为*等价*或*相等*，记作

$$P(p,q,\cdots)\equiv Q(p,q,\cdots),$$

如果它们具有相同的真值表. 例如，命题 $\neg(p\wedge q)$ 与 $\neg p\vee\neg q$ 的真值表如图 4－6. 它们的真值表是相同的，即每个命题都是在第一种情况为假，而其余三种情况为真. 由此，我们可以写

$$\neg(p\wedge q)\equiv\neg p\vee\neg q.$$

换言之，这两个命题是逻辑等价的.

p	q	$p\wedge q$	$\neg(p\wedge q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

(a) $\neg(p\wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p\vee\neg q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

(b) $\neg p\vee\neg q$

图 4－6

注 考察陈述语句

“玫瑰是红的与紫罗兰是蓝的是错误的”.

这一语句可以用符号写为：$\neg(p\wedge q)$，其中

p：“玫瑰是红的” q：“紫罗兰是蓝的”

但是如上所述，$\neg(p\wedge q)\equiv\neg p\vee\neg q$. 于是陈述语句

“玫瑰不是红的，或紫罗兰不是蓝的”

与前面的语句具有相同的意义.

4.7 命题代数

命题满足的各种定律列于表 4－1.（在该表中，T 和 F 分别表示真值表中的“真”和“假”.）我们将这些正式叙述为下面的定理.

定理 4.2 命题满足表 4－1 中的定律.

表 4－1 命题的代数定律

幂等律	
(1a) $p\vee p\equiv p$	(1b) $p\wedge p\equiv p$
结合律	
(2a) $(p\vee q)\vee r\equiv p\vee(q\vee r)$	(2b) $(p\wedge q)\wedge r\equiv p\wedge(q\wedge r)$
交换律	
(3a) $p\vee q\equiv q\vee p$	(3b) $p\wedge q\equiv q\wedge p$
分配律	
(4a) $p\vee(q\wedge r)\equiv(p\vee q)\wedge(p\vee r)$	(4b) $p\wedge(q\vee r)\equiv(p\wedge q)\vee(p\wedge r)$
同一律	
(5a) $p\vee \mathrm{T}\equiv p$	(5b) $p\wedge \mathrm{F}\equiv p$
(6a) $p\vee \mathrm{T}\equiv \mathrm{T}$	(6b) $p\wedge \mathrm{F}\equiv \mathrm{F}$
互补律	
(7a) $p\vee\neg p\equiv \mathrm{T}$	(7b) $p\wedge\neg p\equiv \mathrm{F}$
(8a) $\neg \mathrm{T}\equiv \mathrm{F}$	(8b) $\neg \mathrm{F}\equiv \mathrm{T}$
对合律	
(9) $\neg\neg p\equiv p$	
DeMorgan 律	
(10a) $\neg(p\vee q)\equiv\neg p\wedge\neg q$	(10b) $\neg(p\wedge q)\equiv\neg p\vee\neg q$

4.8 条件语句和双条件语句

许多语句具有形式“如果 p 则 q”，尤其在数学中更是如此. 这样的语句称为条件语句，记作

$$p \to q.$$

条件 $p \to q$ 常读作"p 蕴含 q"或者"仅当 q 时有 p".

另一个常用的语句形式为"p 当且仅当 q". 这样的语句称为双条件语句,记作

$$p \leftrightarrow q.$$

$p \to q$ 与 $p \leftrightarrow q$ 的真值由图 4-7 的表定义. 注意到

(a) 条件 $p \to q$ 为假仅当第一部分 p 为真而第二部分 q 为假. 由此,当 p 为假时,无论 q 的真值如何,条件 $p \to q$ 都为真.

(b) 只要 p 与 q 的真值相同,双条件 $p \leftrightarrow q$ 即为真,否则为假.

图 4-8 给出了命题 $\neg p \vee q$ 的真值表. 注意到 $\neg p \vee q$ 的真值表与 $p \to q$ 的真值表相同,即它们都只有第二种情况为假. 因此 $p \to q$ 与 $\neg p \vee q$ 逻辑等价. 即

$$p \to q \equiv \neg p \vee q.$$

换句话说,语句"如果 p 则 q"与"非 p 或 q"逻辑等价,它们仅涉及到的联结词 $\vee$ 与 $\neg$ 已经是我们的语言之部分. 我们可以把 $p \to q$ 作为某些频繁使用语句的一个缩写.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

(a) $p \to q$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

(b) $p \leftrightarrow q$

图 4-7

p	q	$\neg p$	$\neg p \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

$\neg p \vee q$

图 4-8

4.9 论　证

论证是一个断言,是从称为前提的给定命题集合 $P_1, P_2, \cdots, P_n$ 推出称为结论的另一个命题 Q 的过程. 这样的论证记作

$$P_1, P_2, \cdots, P_n \vdash Q.$$

"逻辑论证"或"有效论证"的概念定义如下.

定义 4.4　一个论证 $P_1, P_2, \cdots, P_n \vdash Q$ 称为有效的,如果前提 $P_1, P_2, \cdots, P_n$ 为真则 Q 为真.

无效的论证称为谬误.

例 4.5　(a) 下面的论证是有效的:

$$p, p \to q \vdash q \quad \textbf{(拆分律)}.$$

这个法则的证明由图 4-9 的真值表可得. 特别地,p 与 $p \to q$ 同时为真只有第一行,而此时 q 为真.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

图 4-9

(b) 下面的论证是谬误的:

$$p \to q, q \vdash p.$$

图 4-9 的真值表的第三行为 $p \to q$ 与 q 皆为真,但是此时 p 为假.

命题 $P_1, P_2, \cdots, P_n$ 同时为真当且仅当命题 $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ 为真. 于是论证 $P_1, P_2, \cdots, P_n \vdash Q$ 有效当且仅当只要 $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ 为真就有 Q 为真,或者等价地,如果命题 $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \to Q$ 为永真命题. 这可以归纳为下面的定理.

定理 4.3　论证 $(P_1, P_2, \cdots, P_n) \vdash Q$ 有效当且仅当命题 $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \to Q$ 是一个永真命题.

下面为本定理应用的例子.

例 4.6　逻辑推理叙述的一个基本原理为

"如果 p 蕴含 q 且 q 蕴含 r,则 p 蕴含 r"

也就是说，下列论证有效

$$p \to q, q \to r \vdash p \to r \qquad \text{（三段论律）.}$$

这个事实由图 4-10 的真值表验证，它说明命题

$$[(p \to q) \land (q \to r)] \to (p \to r)$$

是一个永真命题.等价地，因为前提 $p \to q$ 与 $q \to r$ 同时为真仅出现于第 1,5,7,8 行，而在这些行中结论 $p \to r$ 都为真.（注意，因为共有三个变量 p,q,r，所以真值表有 $2^3=8$ 行.）

我们现在利用上述理论来进行一些特殊陈述的论证.我们强调论证是否有效与真值表以及论证中的陈述内容都没有关系，但是却与论证的形式有关.下例将说明这点.

p	q	r	$[(p$	$\to$	$q)$	$\land$	$(q$	$\to$	$r)]$	$\to$	$(p$	$\to$	$r)$
T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T	F	F	T	T	F	F
T	F	T	T	F	F	F	F	T	T	T	T	T	T
T	F	F	T	F	F	F	F	T	F	T	T	F	F
F	T	T	F	T	T	T	T	T	T	T	F	T	T
F	T	F	F	T	T	F	T	F	F	T	F	T	F
F	F	T	F	T	F	T	F	T	T	T	F	T	T
F	F	F	F	T	F	T	F	T	F	T	F	T	F
步骤			1	2	1	3	1	2	1	4	1	2	1

图 4-10

例 4.7 考虑下列陈述语句

S_1： 如果一个人是单身汉，则他是不幸福的.

S_2： 如果一个人不幸福，则这个人死得早.

S： 单身汉死得早.

这里，横线下面的 S 为论证的结论，而横线上面的 S_1,S_2 为前提.我们断言论证 $S_1,S_2 \vdash S$是有效的.对于论证形式

$$p \to q, q \to r \vdash p \to r,$$

p 为“他是单身汉”，q 为“他不幸福”而 r 为“他死得早”.根据例 4.6，这个论证（三段论律）是有效的.

4.10 逻辑蕴含

称命题 $P(p,q,\cdots)$逻辑蕴含命题 $Q(p,q,\cdots)$，记作

$$P(p,q,\cdots) \Rightarrow Q(p,q,\cdots).$$

即若 $P(p,q,\cdots)$为真，必有 $Q(p,q,\cdots)$为真.

例 4.8 我们断言 p 逻辑蕴含 $p \land q$.观察图 4-11 的真值表可见，对于 p 为真的第 1,2 行，$p \land q$ 也为真.于是 $p \Rightarrow p \land q$.

p	q	$p \lor q$
T	T	T
T	F	T
F	T	T
F	F	F

图 4-11

现在，由 $P(p,q,\cdots)$为真，就必有 $Q(p,q,\cdots)$为真，可以推知论证

$$P(p,q,\cdots) \vdash Q(p,q,\cdots)$$

有效，反之亦然.也就是说，论证 $P \vdash Q$ 有效当且仅当陈述 $P \to Q$ 永真命题.这可以归纳为下述定理.

定理 4.4 对于任意的命题 $P(p,q,\cdots)$与 $Q(p,q,\cdots)$，下列三个陈述等价：

(i) $P(p,q,\cdots)$逻辑蕴含 $Q(p,q,\cdots)$.

(ii) 论证 $P(p,q,\cdots) \vdash Q(p,q,\cdots)$有效.

(iii) 命题 $P(p,q,\cdots)\to Q(p,q,\cdots)$是一个永真命题.

有些逻辑学者和许多课本用"蕴含"一词代替这里的"逻辑蕴含",因此他们就要区分"蕴含"与"如果…那么",事实上,其区别由上述定理可以立即看出.

4.11　命题函数,量词

设 A 为一个给定集合. 定义于 A 上的一个*命题函数*(或称为*开放语句*或*开放条件*)是一个表达式

$$p(x),$$

满足对每个 $a\in A$, $p(a)$或为真或为假. 即以任意的 $a\in A$ 向 x 赋值时,$p(x)$都成为一个陈述(具有其真值). 集合 A 称为 $p(x)$的*定义域*,而 A 中所有使得 $p(a)$为真的元素的集合 T_p 称为 $p(x)$的*真集*. 换句话说,

$$T_p=\{x:x\in A,p(x)\text{ 为真}\}\quad\text{或}\quad T_p=\{x:p(x)\}.$$

当 A 为数的集合时,条件 $p(x)$通常是一个关于变量 x 的等式或不等式方程.

例 4.9　求定义于正整数集 **N** 上的命题函数 $p(x)$的真集.

(a) 设 $p(x)$为"$x+2>7$". 则其真集为

$$\{x:x\in \mathbf{N},x+2>7\}=\{6,7,8,\cdots\}.$$

即大于 5 的所有整数的集合.

(b) 设 $p(x)$为"$x+5<3$". 则其真集为

$$\{x:x\in \mathbf{N},x+5<3\}=\varnothing.$$

换句话说,对于 **N** 中的任意整数,$p(x)$不真.

(c) 设 $p(x)$为"$x+5>1$". 则其真集为

$$\{x:x\in \mathbf{N},x+5>1\}=\mathbf{N}.$$

即对于 **N** 中的任意元素,$p(x)$为真.

注　上例说明,如果 $p(x)$为定义于集合 A 上的命题函数,则 $p(x)$可能对所有的 $a\in A$ 为真,也可能对某些 $a\in A$ 为真,也可能对任意 $a\in A$ 都不真.

下面两小节讨论与这些命题函数有关的量词问题.

全称量词

设 $p(x)$为定义于集合 A 上的命题函数. 考虑表达式

$$(\forall x\in A)p(x)\quad\text{或}\quad \forall x\,p(x), \tag{4.1}$$

读作"对 A 中的每个 x, $p(x)$为真语句",或简单地,"对所有 x,$p(x)$". 符号

$$\forall$$

读作"对所有"或"对每个",称为*全称量词*. 表达式(4.1)等价于

$$T_p=\{x:x\in A,p(x)\}=A, \tag{4.2}$$

即 $p(x)$的真集是整个 A.

表达式 $p(x)$自身是一个开放语句或开放条件,因而不具有真值. 然而,$\forall x\,p(x)$,即由(4.1)或(4.2),在 $p(x)$之前加上量词$\forall$之后,就立即具有一个真值了. 特别地,

Q_1:　如果$\{x:x\in A,p(x)\}=A$,则$\forall x\,p(x)$为真;否则$\forall x\,p(x)$为假.

例 4.10　(a) 命题$(\forall n\in \mathbf{N})(n+4>3)$为真. 因为

$$\{n : n+4>3\}=\{1,2,3,\cdots\}=\mathbf{N}.$$

(b) 命题$(\forall n\in \mathbf{N})(n+2>8)$为假. 因为

$$\{n : n+2>8\}=\{7,8,\cdots\}\neq \mathbf{N}.$$

(c) 对于集合 A_i 的指标类$\{A_i : i\in I\}$. 我们可以应用符号$\forall$来定义其交集，如下，

$$\bigcap (A_i : i\in I)=\{x : \forall i\in I, x\in A_i\}.$$

存在量词

设 $p(x)$为定义于集合 A 上的一个命题函数. 考虑表达式

$$(\exists x\in A)p(x)\quad 或 \quad \exists x, p(x) \tag{4.3}$$

读作“在 A 中存在 x 使得 $p(x)$为真语句”，或简单地，“对某 x，$p(x)$”. 记号

$$\exists$$

读作“存在”或“对某个”或“对于至少一个”，叫做*存在量词*. 陈述(4.3)等价于

$$T_p=\{x : x\in A, p(x)\}\neq\varnothing,$$

即 $p(x)$的真集非空. 由此，在 $p(x)$前加上量词$\exists$，命题$\exists x p(x)$就立即具有真值. 特别地，

> Q_2：　如果$\{x : p(x)\}\neq\varnothing$，则$\exists x\, p(x)$为真；否则$\exists x\, p(x)$为假.

例 4.11　(a) 命题$(\exists n\in \mathbf{N})(n+4<7)$为真. 因为

$$\{n : n+4<7\}=\{1,2\}\neq\varnothing.$$

(b) 命题$(\exists n\in \mathbf{N})(n+6<4)$为假. 因为

$$\{n : n+6<4\}=\varnothing.$$

(c) 对于集合 A_i 的指标类$\{A_i : i\in I\}$. 我们可以应用符号$\exists$来定义其并集，如下，

$$\bigcup (A_i : i\in I)=\{x : \exists i\in I, x\in A_i\}.$$

记号

设 $A=\{2,3,5\}$并设 $p(x)$为语句“x 为一个素数”，或简单地说“x 为素数”. 则

$$2 是素数与 3 是素数与 5 是素数 \tag{*}$$

可以记为

$$p(2)\wedge p(3)\wedge p(5)\quad 或 \quad \wedge(a\in A, p(a)),$$

这等价于语句

$$“A 中的每个数为素数”\quad 或 \quad \forall a\in A, p(a). \tag{**}$$

类似地，命题

“2 是素数或 3 是素数或 5 是素数”

可以记为

$$p(2)\vee p(3)\vee p(5)\quad 或 \quad \vee(a\in A, p(a)),$$

这等价于语句

$$“A 中至少有一个数为素数”\quad 或 \quad \exists a\in A, p(a).$$

换句话说，

$$\wedge(a\in A, p(a))\equiv\forall a\in A, p(a)\quad 且\ \vee(a\in A, p(a))\equiv\exists a\in A, p(a).$$

于是，有时可以用符号$\wedge$和$\vee$代替符号$\forall$和$\exists$.

注　如果 A 是无限集，则语句(*)不能给出，因为该语句不能穷尽；但是形如(**)的语

句总是可行的，甚至对于无限集也是如此.

4.12　量词语句的否定

考虑语句“数学专业的所有学生都是男性”. 其否定为

“数学专业的所有学生都是男性是不对的”

或者等价地

“至少存在一个数学专业学生是女性(非男性)”.

记 M 表示数学专业学生，上述语句可用符号表示为

$$\neg(\forall x \in M)(x\text{ 为男性}) \equiv (\exists x \in M)(x\text{ 非男性}).$$

进而，记 $p(x)$ 表示“x 是男性”，有

$$\neg(\forall x \in M)p(x) \equiv (\exists x \in M)\neg\, p(x) \quad 或 \quad \neg\ \forall x p(x) \equiv \exists x \neg\, p(x).$$

事实上，上述对于任意命题 $p(x)$ 为真，即有下述定理.

定理 4.5(DeMorgan)　$\neg(\forall x \in A)p(x) \equiv (\exists x \in A)\neg\, p(x)$.

换句话说，下面两个语句等价：

(1) 对所有的 $a \in A$，$p(a)$ 为真是不对的.

(2) 存在 $a \in A$ 使得 $p(a)$ 为假.

关于含有存在量词的否定命题还有下面一个类似的定理.

定理 4.6 (DeMorgan)　$\neg(\exists x \in A)p(x) \equiv (\forall x \in A)\neg\, p(x)$.

也就是说，下列两个语句等价：

(1) 对某个 $a \in A$，$p(a)$ 为真是不对的.

(2) 对所有 $a \in A$，$p(a)$ 为假.

例 4.12　(a) 下列语句互为否定.

“对所有正整数 n 有 $n+2>8$”.

“存在一个正整数 n 使得 $n+2 \not> 8$”.

(b) 下列语句互为否定.

“存在一个人(活着的)年龄为 150 岁”.

“每一个活着的人都不是 150 岁”.

注　表达式 $\neg\, p(x)$ 的意义是显然的，即

“当 $p(a)$ 为假时，$\neg\, p(a)$ 为真. 反之亦然”.

显然，$\neg$ 是作用于语句上的运算，这里 $\neg$ 用来作为作用于命题函数上的运算. 类似地，“$p(x) \wedge q(x)$”读作“$p(x)$ 与 $q(x)$”，定义为

“当 $p(a)$ 与 $q(a)$ 均为真时，语句 $P(a) \wedge q(a)$ 为真”.

类似地，“$p(x) \vee q(x)$”读作“$p(x)$ 或 $q(x)$”，定义为

“当 $p(a)$ 或 $q(a)$ 为真时，语句 $P(a) \wedge q(a)$ 为真”.

于是，在真集意义下，我们有

(i) $\neg\, p(x)$ 为 $p(x)$ 的补集.

(ii) $p(x) \wedge q(x)$ 为 $p(x)$ 与 $q(x)$ 的交集.

(iii) $p(x) \vee q(x)$ 为 $p(x)$ 与 $q(x)$ 的并集.

我们可以证明关于命题的运算定律对于命题函数同样成立. 例如 DeMorgan 律：

$$\neg(p(x) \wedge q(x)) \equiv \neg\, p(x) \vee \neg\, q(x) \quad 及$$

$$\neg(p(x) \vee q(x)) \equiv \neg\, p(x) \wedge \neg\, q(x).$$

反例

定理 4.6 告诉我们，证明语句 $\forall x, p(x)$ 为假，可以等价地证明 $\exists x \neg p(x)$ 为真. 换句话说，即存在元素 x_0 使得 $p(x_0)$ 为假. 这样的元素 x_0 称为 $\forall x, p(x)$ 的一个*反例*.

例 4.13 (a) 考虑语句 $\forall x \in \mathbf{R}, |x| \neq 0$. 该语句为假，因为 0 是其一个反例，即 $|0| \neq 0$ 不真.

(b) 考虑语句 $\forall x \in \mathbf{R}, x^2 \geqslant x$. 此语句为假，例如 $\frac{1}{2}$ 为一个反例. 确切地，$\left(\frac{1}{2}\right)^2 \geqslant \frac{1}{2}$ 非真，即 $\left(\frac{1}{2}\right)^2 < \frac{1}{2}$.

(c) 考虑语句 $\forall x \in \mathbf{N}, x^2 \geqslant x$. 此语句为真，因为 $\mathbf{N}$ 为正整数集. 换句话说，不存在正整数 n 使得 $n^2 < n$.

含有多个变量的命题函数

定义于集合 $A = A_1 \times A_2 \times \cdots \times A_n$ 上(含有 n 个变量)的命题函数为一个表达式

$$p(x_1, x_2, \cdots, x_n),$$

满足对于任意的 n 元组 $(a_1, \cdots, a_n)$，$p(a_1, a_2, \cdots, a_n)$ 或者为真或者为假. 例如

$$x + 2y + 3z < 18$$

为 $\mathbf{N}^3 = \mathbf{N} \times \mathbf{N} \times \mathbf{N}$ 上的一个命题函数. 这样的一个命题函数没有真值表. 然而，我们有下述原理.

基本原理 对其每个变量冠以量词后的命题函数为一个语句并且具有真值. 例如

$$\forall x \exists y, p(x,y) \quad \text{或} \quad \exists x\ \exists y\ \exists z, p(x,y,z)$$

为具有真值的语句.

例 4.14 设 $B = \{1,2,3,\cdots,9\}$ 且 $p(x,y)$ 表示"$x+y=10$". 则 $p(x,y)$ 为 $A = B^2 = B \times B$ 上的一个命题函数.

(a) 因为下面语句中每个变量都被冠以量词，所以是命题：

$$\forall x \exists y, p(x,y), \quad \text{即} \quad \text{“对每个 } x\text{，存在 } y \text{ 使得 } x + y = 10\text{”},$$

该命题为真. 例如，若 $x=1$，则有 $y=9$；若 $x=2$，则有 $y=8$，等等.

(b) 下面也是命题：

$$\exists y \forall x, p(x,y), \quad \text{即} \quad \text{“存在 } y \text{ 使得对每个 } x \text{ 有 } x + y = 10\text{”}.$$

显然没有这样的 y 存在，因此命题为假.

注意(a)与(b)之间的惟一区别是量词的次序不同. 于是改变量词的次序可能导致不同的结果. 此外，当把量词语句翻译成语言时，"使得"经常随"存在"而出现.

多变量的否定量词语句

相继地使用定理 4.5 和 4.6，可以得到多变量的否定量词语句. 具体做法是，将否定符号从左向右移动，同时将每个 $\forall$ 换成 $\exists$ 而将每个 $\exists$ 换成 $\forall$. 例如

$$\begin{aligned} \neg[\forall x \exists y \exists z, p(x,y,z)] &\equiv \exists x \neg[\exists y \exists z, p(x,y,z)] \\ &\equiv \exists x \forall y \neg[\exists z, p(x,y,z)] \\ &\equiv \exists x \forall y \forall z \neg p(x,y,z). \end{aligned}$$

做否定量词语句的实际操作时，我们往往不必写出每一个步骤.

例 4.15 (a) 考虑量词语句

"每个学生至少有一门课由助教讲授".

其否定是

"存在一个学生使得他的每一门课都不是由助教讲授".

(b) L 是序列 $a_1, a_2, \cdots$ 的极限的定义为

$$\forall \varepsilon > 0, \exists n_0 \in \mathbf{N}, \forall n > n_0, |a_n - L| < \varepsilon.$$

于是 L 不是序列 $a_1, a_2, \cdots$ 的极限定义为

$$\exists \varepsilon > 0, \forall n_0 \in \mathbf{N}, \exists n > n_0, |a_n - L| \geqslant \varepsilon.$$

问题与解答

命题与逻辑运算

4.1 设 p 为"天冷"，q 为"天下雨". 请用简单的语句描述下列陈述：

(a) $\neg p$;　(b) $p \wedge q$;　(c) $p \vee q$;　(d) $q \wedge \neg p$.

解 ☞ 对于每一种情况，将 $\wedge$，$\vee$，$\neg$ 分别翻译为"与"，"或"，"是错的"或"否"，然后构成日常语句.

(a) 天不冷.　(b) 天冷而且下雨.

(c) 天冷或者天下雨.　(d) 天下雨或天不冷.

4.2 设 p 为"Erik 阅读《新闻周刊》"，q 为"Erik 阅读《纽约人》"，r 为"Erik 阅读《时报》". 将下列陈述用符号表示：

(a) Erik 阅读《新闻周刊》或《纽约人》，但是不阅读《时报》.

(b) Erik 阅读《新闻周刊》与《纽约人》，或者他不阅读《新闻周刊》与《时报》.

(c) Erik 阅读《新闻周刊》不阅读《时报》是错的.

(d) Erik 阅读《时报》或《纽约人》，但是不阅读《新闻周刊》是错的.

解 ☞ 分别用 $\vee$，$\wedge$ 表示"或"，"与"(或者其逻辑等价用语"但是")，用 $\neg$ 表示"非"(否定).

(a) $(p \vee q) \wedge \neg r$.　(b) $(p \wedge q) \vee \neg (p \wedge q)$.

(c) $\neg (p \wedge \neg r)$.　(d) $\neg [(r \vee q) \wedge \neg p]$.

真值与真值表

4.3 试确定下列陈述的真值.

(a) $4+2=5$ 与 $6+3=9$.　(b) $3+2=5$ 与 $6+1=7$.

(c) $4+5=9$ 与 $1+2=4$.　(d) $3+2=5$ 与 $4+7=11$.

解 ☞ 陈述"p 与 q"为真仅当两者同时为真. 因此(a)假；(b)真；(c) 假；(d)真.

4.4 求 $\neg p \wedge q$ 的真值表.

解 ☞ 构造真值表的两种方式如图 4-12 所示.

p	q	$\neg p$	$\neg p \wedge q$
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

(a) 法一

p	q	$\neg$	p	$\wedge$	q
T	T	F	T	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	F	F	F
步骤		2	1	3	1

(b) 法二

图 4-12

4.5 验证命题 $p \vee \neg (p \wedge q)$ 为一个永真命题.

证 ☞ 如图 4-13，构造出 $p \vee \neg (p \wedge q)$ 的真值表. 因为对于 p 和 q 的所有值，$p \vee \neg (p \wedge q)$ 的真值均为 T，所以此命题为一个永真命题.

p	q	$p\wedge q$	$\neg(p\wedge q)$	$p\vee\neg(p\wedge q)$
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

图 4 - 13

4.6　证明命题$\neg(p\wedge q)$与$\neg p\vee\neg q$逻辑等价.

证 ☞　如图 4 - 14,构造出$\neg(p\wedge q)$与$\neg p\vee\neg q$的真值表. 因为真值表相同(都在第一行为假而其余行为真),所以命题$\neg(p\wedge q)$与$\neg p\vee\neg q$逻辑等价. 因此可以写

$$\neg(p\wedge q)\equiv\neg p\vee\neg q.$$

p	q	$p\wedge q$	$\neg(p\wedge q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

(a)　$\neg(p\wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p\vee\neg q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

(b)　$\neg p\vee\neg q$

图 4 - 14

4.7　试应用表 4 - 1 中的定律证明$\neg(p\vee q)\vee(\neg p\wedge q)\equiv\neg p$.

证 ☞

	陈述	理由
(1)	$\neg(p\vee q)\vee(\neg p\wedge q)\equiv(\neg p\wedge\neg q)\vee(\neg p\wedge q)$	DeMorgan 律
(2)	$\equiv\neg p\wedge(\neg q\vee q)$	分配律
(3)	$\equiv\neg p\wedge T$	互补律
(4)	$\equiv\neg p$	恒等律

条件语句

4.8　不用条件语句,重述下列陈述.

(a) 如果天气冷,他就戴帽子.

(b) 如果增产,就加工资.

解 ☞　回忆"如果 p 则 q"等价于"非 p 或 q",即 $p\to q\equiv\neg p\vee q$. 因此,

(a) 天气不冷或者他戴帽子.

(b) 不增产或者加工资.

4.9　写出下列陈述的逆否命题:

(a) 如果 John 是诗人,则他贫穷.

(b) Marc 想要通过考试,就得学习.

解 ☞　(a) $p\to q$ 的逆否命题是$\neg q\to\neg p$. 因此题给陈述的逆否命题为

如果 John 不贫穷,则他不是诗人.

(b) 所给陈述的等价说法是"如果 Marc 通过考试,则他学习了". 因此有逆否命题

如果 Marc 不学习,他将不会通过考试.

4.10　考虑条件命题 $p\to q$. 命题 $q\to p$, $\neg p\to\neg q$, $\neg q\to\neg p$ 分别称为 $p\to q$ 的逆命题,否命题,逆否命题. 问这些命题中何者逻辑等价于命题 $p\to q$?

解 ☞　构造这些命题的真值表如图 4 - 15. 只有逆否命题$\neg q\to\neg p$ 与原命题 $p\to q$ 等价.

p	q	$\neg p$	$\neg q$	条件 $p\rightarrow q$	逆 $q\rightarrow p$	否 $\neg p\rightarrow\neg q$	逆　否 $\neg q\rightarrow\neg p$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

图 4－15

4.11 尽可能简单地写出下列命题的否定命题.

(a) 如果她工作,她就能赚钱.

(b) 他游泳当且仅当水温暖.

(c) 如果天下雪,他们就不开汽车.

解答 (a) 注意到$\neg(p\rightarrow q)\equiv p\wedge\neg q$,因此题给陈述的否定为

她工作或者她不赚钱.

(b) 注意到$\neg(p\leftrightarrow q)\equiv p\leftrightarrow\neg q\equiv\neg p\leftrightarrow q$,因此下述两个陈述都是题给陈述的否定.

他游泳当且仅当水不暖.

他不游泳当且仅当水暖.

(c) 注意到$\neg(p\rightarrow\neg q)\equiv p\wedge\neg\neg q\equiv p\wedge q$. 因此题给陈述的否定是

天下雪与他们开车.

论证

4.12 证明论证 $p\rightarrow q,\neg p\vdash\neg q$ 为谬误.

证明 构造$[(p\rightarrow q)\wedge\neg p]\rightarrow\neg q$的真值表如图 4－16. 因为命题$[(p\rightarrow q)\wedge\neg p]\rightarrow\neg q$不是永真命题,所以为谬误. 等价地,因为真值表的第三行$p\rightarrow q$与$\neg p$为真,但是$\neg q$为假,故该论证为谬误.

p	q	$p\rightarrow q$	$\neg p$	$(p\rightarrow q)\wedge\neg p$	$\neg q$	$[(p\rightarrow q)\wedge\neg p]\rightarrow\neg q$
T	T	T	F	F	F	T
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T

图 4－16

4.13 判定论证 $p\rightarrow q,\neg q\vdash\neg p$ 为有效.

解答 构造 $p\rightarrow q,\neg q\vdash\neg p$ 的真值表如图 4－17. 因为命题 $p\rightarrow q,\neg q\rightarrow\neg p$ 为永真命题,所以该论证有效.

p	q	$[(p$	$\rightarrow$	$q)$	$\wedge$	$\neg$	$q]$	$\rightarrow$	$\neg$	p
T	T	T	T	T	F	F	T	T	F	T
T	F	T	F	F	F	T	F	T	F	T
F	T	F	T	T	F	F	T	T	T	F
F	F	F	T	F	T	T	F	T	T	F
步骤		1	2	1	3	2	1	4	2	1

图 4－17

4.14 证明论证 $p\rightarrow\neg q,r\rightarrow q,r\vdash\neg p$ 为有效.

证明 构造出该论证的前提与结论的真值表如图 4－18. $p\rightarrow\neg q,r\rightarrow q$ 与 r 同时为真只在真值表的第五行中出现,而此时$\neg p$也为真,所以论证有效.

	p	q	r	$p\to\neg q$	$r\to q$	$\neg q$
1	T	T	T	F	T	F
2	T	T	F	F	T	F
3	T	F	T	T	F	F
4	T	F	F	T	T	F
5	F	T	T	T	T	T
6	F	T	F	T	T	T
7	F	F	T	T	F	T
8	F	F	F	T	T	T

图 4 - 18

4.15 验证下述论证是否有效.

如果三角形的两边相等,则其所对的角相等.
一个三角形的两边不相等.

这两边的对角不相等.

证 ☞　首先将论证翻译为符号形式:$p\to q,\neg p\vdash\neg q$,其中,$p$ 为"三角形中有两边相等",q 为"所对的角相等".由问题 4.12,此论证为谬误.

注　尽管根据欧几里得公理和前提二,结论确实成立,但是上述不能构成这一结论的证明,因为它是一个谬误.

4.16 试说明下列论证是否有效.

如果 7 小于 4,那么 7 不是一个素数.
7 不小于 4.

---

7 是一个素数.

证 ☞　首先将论证过程翻译为符号形式.设 p 表示"7 小于 4",q 表示"7 是一个素数".则题给论证为

$$p\to\neg q,\neg p\vdash q.$$

构造真值表如图 4 - 19.真值表显示上述论证为谬误.因为在第四行,前提 $p\to\neg q$ 与 $\neg p$ 为真,但是结论 q 为假.

注　要证明的结论事实上为真与这个论证为谬误没有关系.

p	q	$\neg q$	$p\to\neg q$	$\neg p$
T	T	F	F	F
T	F	T	T	F
F	T	F	T	T
F	F	T	T	T

图 4 - 19

量词与命题函数

4.17 设 $A=\{1,2,3,4,5\}$.试确定下述陈述语句的真值.

(a) $(\exists x\in A)(x+3=10)$.　　(b) $(\forall x\in A)(x+3<10)$.

(c) $(\exists x\in A)(x+3<5)$.　　(d) $(\forall x\in A)(x+3\leqslant 7)$.

解 ☞　(a) 假.因为 A 中没有一个数是 $x+3=10$ 的解.

(b) 真.A 中每个数都满足 $x+3<10$.

(c) 真.因为若 $x_0=1$,则 $x_0+3<5$,即 1 为一个解.

(d) 假.因为若 $x_0=5$,则 x_0+3 不小于等于 7.换言之,5 不是给定条件的解.

4.18 确定下列陈述语句的真值.其中 $U=\{1,2,3\}$ 为全集.

(a) $\exists x\ \forall y, x^2<y+1$.

(b) $\forall x\ \exists y, x^2+y^2<12$.

(c) $\forall x\ \forall y, x^2+y^2<12$.

解 (a) 真. 比如设 $x=1$,则 1,2,3 都是 $1<y+1$ 的解.

(b) 真. 因为对每个 x_0 可设 $y=1$,则 ${x_0}^2+1<12$ 为真命题.

(c) 假. 因为若 $x_0=2$ 且 $y_0=3$,则 ${x_0}^2+{y_0}^2<12$ 不是一个真命题.

4.19 否定下列每个陈述语句.

(a) $\exists x\ \forall y, p(x,y)$.

(b) $\exists x\ \forall y, p(x,y)$.

(c) $\exists y\ \exists x\ \exists z, p(x,y,z)$.

解 利用 $\neg\ \forall x\, p(x)\equiv\exists x \neg\ p(x)$ 与 $\neg\ \exists x\, p(x)\equiv\forall x\neg\ p(x)$.

(a) $\neg(\exists x\ \forall y, p(x,y))\equiv\forall x\exists y\neg\ p(x,y)$.

(b) $\neg(\forall x\ \forall y, p(x,y))\equiv\exists x\exists y\neg\ p(x,y)$.

(c) $\neg(\exists y\ \exists x\ \forall z, p(x,y,z))\equiv\forall y\forall x\exists z\neg\ p(x,y,z)$.

4.20 设 $p(x)$ 表示"$x+2>5$". 说明对于下列每个集合,$p(x)$ 是否为其上的命题函数.

(a) 正整数集合 **N**.

(b) $M=\{-1,-2,-3,\cdots\}$.

(c) 复数集 **C**.

解 (a) 是.

(b) 尽管对 M 中每个元素 $p(x)$ 均为假,但 $p(x)$ 仍然为 M 上的一个命题函数.

(c) 不是. 因为 $2i+2>5$ 没有意义,换言之,该不等式在复数集中不成立.

4.21 否定下列陈述语句.

(a) 所有学生都住在宿舍中.

(b) 所有数学专业的学生都是男性.

(c) 一些学生为 25 岁及其以上年纪.

解 利用定理 4.5 来否定陈述语句中的量词.

(a) 至少有一个学生不住在宿舍中(有些学生不住在宿舍中).

(b) 至少有一个数学专业的学生是女性(数学专业有些学生是女性).

(c) 没有哪个学生为 25 岁及其以上年纪(所有学生都小于 25 岁).

补　充　题

命题与逻辑运算

4.22 设 p 为"Audrey 讲法语",q 为"Audrey 讲丹麦语". 请用简单口语描述下列命题.

(a) $p\vee q$.　(b) $p\wedge q$.　(c) $p\wedge\neg\ q$.　(d) $\neg\ p\vee\neg\ q$　(e) $\neg\neg\ p$.

(f) $\neg(\neg\ p\wedge\neg\ q)$.

4.23 设 p 表示"他富有",q 表示"他幸福". 以 $\neg\ p$ 和 $\neg\ q$ 分别表示"他贫穷"和"他不幸福". 请用 p,q 将下列陈述符号化.

(a) 如果他富有,那么他不幸福.

(b) 他既不富有也不幸福.

(c) 要幸福必须贫穷.

(d) 贫穷就不幸福.

4.24 求真值表:(a) $p\vee\neg\ q$.　(b) $\neg\ p\wedge\neg\ q$.

4.25 验证命题 $(p\wedge q)\wedge\neg(p\vee q)$ 为一个永假命题.

论证

4.26 验证下列论证是否有效.

(a)

如果下雨,Erik 就要生病.
天没有下雨.

Erik 没有生病.

(b)

如果下雨,Erik 就要生病.
Erik 没有生病.

天没有下雨.

4.27 验证下列论证是否有效.

如果我学习,我的数学课就不会不及格.
如果我不打篮球,我就会学习.
但是我的数学课不及格.

因此我肯定打篮球了.

4.28 证明:

(a) $p\wedge q$ 逻辑蕴含 $p\leftrightarrow q$.

(b) $p\leftrightarrow\neg q$ 不逻辑蕴含 $p\rightarrow q$.

量词

4.29 设 $A=\{1,2,\cdots,9,10\}$. 考察下列语句,如果是陈述,请确定其真值;如果是命题函数,请确定其真集.

(a) $(\forall x\in A)(\exists y\in A)(x+y<14)$.　　(b) $(\forall y\in A)(x+y<14)$.

(c) $(\forall x\in A)(\forall y\in A)(x+y<14)$.　　(d) $(\exists y\in A)(x+y<14)$.

4.30 否定下列陈述.

(a) 如果老师不在,那么就有些学生不完成作业.

(b) 所有学生完成了作业与老师在场.

(c) 有些学生没有完成作业或老师不在.

4.31 否定问题 4.17 中的每个陈述.

4.32 求每个陈述的反例. 其中 $U=\{3,5,7,9\}$为全集.

(a) $\forall x, x+3\geqslant 7$.　(b) $\forall x$, x 为奇数.　(c) $\forall x$, x 为素数.　(d) $\forall x, |x|=x$.

补充题答案

4.22 将$\wedge$,$\vee$,$\neg$ 分别翻译为"与","或","非"或"是不对的",然后整理为通常的语句.

(a) Audrey 说法语或丹麦语.

(b) Audrey 说法语与丹麦语.

(c) Audrey 说法语但是不说丹麦语.

(d) Audrey 不说法语或她不说丹麦语.

(e) Audrey 不说法语不是事实.

(f) Audrey 既不说法语也不说丹麦语不是事实.

4.23 (a) $p\rightarrow\neg q$.　(b) $\neg p\wedge\neg q$.　(c) $q\rightarrow\neg p$.　(d) $\neg p\leftrightarrow\neg q$.

4.24 真值表见图 4-20.

p	q	$\neg q$	$p\vee\neg q$
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

(a)

p	q	$\neg p$	$\neg q$	$\neg p\wedge\neg q$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

(b)

图 4－20

4.25 因为在图 4－21 的真值表中，对于 p 和 q 的所有值，命题为假，故它是一个永假命题.

p	q	$p\wedge q$	$p\vee q$	$\neg(p\vee q)$	$(p\wedge q)\wedge\neg(p\vee q)$
T	T	T	T	F	F
T	F	F	T	F	F
F	T	F	T	F	F
F	F	F	F	T	F

图 4－21

4.26 首先将论证翻译成符号形式. 设 p 表示“天下雨”，q 表示“Erik 生病”.

(a) $p\to q,\neg p\vdash\neg q$.　　(b) $p\to q,\neg q\vdash\neg p$.

由问题 4.12，论证(a)为谬误，而由问题 4.13，论证(b)有效.

4.27 设 p 表示“我学习”，q 表示“我数学不及格”，r 表示“我打篮球”. 则所给论证为

$$p\to\neg q,\neg r\to p,q\vdash r.$$

构造真值表如图 4－22，其中前提 $p\to\neg q$，$\neg r\to p$ 与 q 同时为真仅在表的第五行出现，而在该行结论 r 也为真，因此论证有效.

p	q	r	$\neg q$	$p\to\neg q$	$\neg r$	$\neg r\to p$
T	T	T	F	F	F	T
T	T	F	F	F	T	T
T	F	T	T	T	F	T
T	F	F	T	T	T	T
F	T	T	F	T	F	T
F	T	F	F	T	T	F
F	F	T	T	T	F	T
F	F	F	T	T	T	F

图 4－22

4.28 (a) 构造 $p\wedge q$ 与 $p\leftrightarrow q$ 的真值表如图 4－23(a). 注意 $p\wedge q$ 仅在第一行为真，而此时 $p\leftrightarrow q$ 也为真.

(b) 构造 $p\leftrightarrow\neg q$ 与 $p\to q$ 的真值表如图 4－23(b). 注意 $p\leftrightarrow\neg q$ 在第二行为真，但是在该行 $p\to q$ 为假.

p	q	$p\wedge q$	$p\leftrightarrow q$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	T

(a)

p	q	$\neg q$	$p\leftrightarrow\neg q$	$p\to q$
T	T	F	F	T
T	F	T	T	F
F	T	F	T	T
F	F	T	F	T

(b)

图 4－23

4.29 (a) 开放语句的两个变量被分别冠以两个量词，因此是一个陈述. 进而，该陈述为真.

(b) 开放语句被冠以一个量词，因此它是其余变量的一个命题函数. 注意到对于每个 $y\in A$，$x_0+y<14$ 当且仅当 $x_0=1,2$，或 3. 因此真集为$\{1,2,3\}$.

(c) 是一个陈述并且为假. 如果 $x_0=8$ 且 $y_0=9$，则 $x_0+y_0<14$ 为假.

(d) 为关于 x 的开放语句. 真集为 A 自身.

4.30 (a) 老师不在与所有学生完成了作业.

(b) 有些学生没有完成作业或者老师不在.

(c) 所有学生完成了作业与老师在场.

4.31 (a) $(\forall x \in A)(x+3 \neq 10)$.

(b) $(\exists x \in A)(x+3 \geqslant 10)$.

(c) $(\forall x \in A)(x-3 \geqslant 5)$.

(d) $(\exists x \in A)(x+3 > 7)$.

4.32 (a) 反例为 5,7,9.

(b) 因为不存在反例,所以陈述为真.

(c) 9 是仅有的反例.

(d) 因为不存在反例,所以陈述为真.

第五章　向量与矩阵

5.1　引　　言

数据通常被排成一张表,也就是说,其元素都带有一个或多个下标.通常将一维数表称为向量,而将二维数表称为矩阵.(这里,维数表示下标的个数.)我们来导出这些概念及其记号.

假设8个学生的体重(磅数)如下：

$$134,\quad 156,\quad 127,\quad 145,\quad 203,\quad 186,\quad 145,\quad 138.$$

我们可以用一个字母,比如 w,加以不同的下标将这些数值列表表示：

$$w_1,\quad w_2,\quad w_3,\quad w_4,\quad w_5,\quad w_6,\quad w_7,\quad w_8.$$

注意到每个下标都表示了该数在表中的位置.例如

$$w_1 = 134,\quad 第一个数;\quad w_2 = 156\quad 第二个数,\quad \cdots$$

这样的一个列表称为**向量**或**线性数表**.

利用下标,我们可以写出和 S 与平均体重 A 如下：

$$S = \sum_{k=1}^{8} w_k = w_1 + w_2 + \cdots + w_8,\qquad A = \frac{S}{8} = \frac{1}{8}\Big[\sum_{k=1}^{8} w_k\Big].$$

为了对一列数的计算进行简洁表达,下标记号是必不可少的.

同样,设有28家连锁店,每个连锁店有4个销售部,我们可以列出他们一周的销售额(近似到美元),如表5-1.我们只需要一个字母,比如 s,加上它的两个下标将这些数值列为一张表：

表5-1

连锁店 \ 销售部	1	2	3	4
1	2872	805	3211	1560
2	2196	1223	2525	1744
3	3257	1017	3686	1951
⋮	⋮	⋮	⋮	⋮
28	2618	931	2333	982

$$s_{1,1}, s_{1,2}, s_{1,3}, s_{1,4}, s_{2,1}, s_{2,2}, \cdots, s_{28,4}.$$

其中 $s_{i,j}$ 表示第 i 个连锁店的第 j 个销售部.(在不会产生混淆时,我们写 s_{ij} 来代替 $s_{i,j}$.)于是

$$s_{11} = \$2872,\quad s_{12} = \$805,\quad s_{13} = \$3211,\quad \cdots.$$

这样的矩形数表称为**矩阵**或**二维数表**.

本章讨论向量,矩阵和一些代数运算.相对于矩阵和向量,数字则被称为**纯量**.

5.2　向　　量

向量 u 是指一列数,如 $a_1, a_2, \cdots, a_n$.记作

$$u = (a_1, a_2, \cdots, a_n).$$

数 a_i 称为 u 的**分量**或**表值**.如果所有的 $a_i=0$,则称 u 为一个**零向量**.两个向量 u 和 v 称为相等的,记作 $u=v$,如果他们的分量个数相同而且对应分量相等.

例5.1　(a) 下列都是向量：

$$(3,-4),\quad (6,8),\quad (0,0,0),\quad (2,3,4).$$

前两个向量具有两个分量,而后两个向量具有三个分量.第三个向量是具有三个分量的零向量.

(b) 尽管向量(1,2,3)与(2,3,1)包含相同的数,但是它们不相等,因为对应分量不

相等.

向量的运算

考虑任意两个分量个数相同的向量 u 和 v. 比如

$$u=(a_1,a_2,\cdots,a_n),\qquad v=(b_1,b_2,\cdots,b_n).$$

则向量 u 与 v 的和,记作 $u+v$,是将 u 与 v 的对应分量相加而得到的向量,即

$$u+v=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n).$$

数 k 乘以向量 u 称为数乘向量或简称数乘,记作 ku,是将数 k 乘以 u 的每一个分量得到的向量,即

$$ku=(ka_1,ka_2,\cdots,ka_n).$$

我们还定义

$$-u=-1(u),\qquad u-v=u+(-v),$$

并设 0 表示零向量. 向量 $-u$ 称为向量 u 的负向量.

向量 u 与 v 的点积或内积定义为

$$u\cdot v=a_1b_1+a_2b_2+\cdots+a_nb_n.$$

向量 u 的范数或长度定义为

$$\| u\| =\sqrt{u\cdot u}=\sqrt{a_1^2+a_2^2+\cdots+a_n^2}.$$

注意,$\| u\| =0$ 当且仅当 $u=0$,否则 $\| u\| >0$.

例 5.2 设 $u=(2,3,-4)$, $v=(1,-5,8)$. 则

$u+v=(2+1,3-5,-4+8)=(3,-2,4)$.

$5u=(5\cdot 2,5\cdot 3,5\cdot(-4))=(10,15,-20)$.

$-v=-1\cdot(1,-5,8)=(-1,5,-8)$.

$2u-3v=(4,6,-8)+(-3,15,-24)=(1,21,-32)$.

$u\cdot v=2\cdot 1+3\cdot(-5)+(-4)\cdot 8=2-15-32=-45$.

$\| u\| =\sqrt{2^2+3^2+(-4)^2}=\sqrt{4+9+16}=\sqrt{29}$.

向量的加法和数乘具有许多性质,比如

$$k(u+v)=ku+kv,$$

其中 k 为纯量而 u,v 为向量. 其余性质将在定理 5.1(对于矩阵)中列出(见5.4),那些性质对向量同样成立,因为向量可以看做特殊的矩阵.

列向量

有时,一列数不是写成水平格式,而是写成竖直格式,这样的格式称为列向量. 相对于此,上述写为水平格式的向量称为行向量. 对于行向量的讨论都可以移植到列向量中.

例 5.3 (a) 下列向量为列向量:

$$\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\-3\end{bmatrix},\begin{bmatrix}1\\2\\-6\end{bmatrix},\begin{bmatrix}1.4\\3/4\\-19\end{bmatrix}.$$

(b) 设

$$u=\begin{bmatrix}5\\3\\-4\end{bmatrix},v=\begin{bmatrix}3\\-1\\-2\end{bmatrix}.$$

则

$$2u-3v=\begin{bmatrix}10\\6\\-8\end{bmatrix}+\begin{bmatrix}-9\\3\\6\end{bmatrix}=\begin{bmatrix}1\\9\\-2\end{bmatrix}.$$

$$u \cdot v = 15 - 3 + 8 = 20.$$
$$\| u \| = \sqrt{25+9+16} = \sqrt{50} = 5\sqrt{2}.$$

5.3 矩 阵

矩阵 A 是一张矩形数表，通常记作

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

其中 m 个水平排列的数表称为矩阵 A 的行，而 n 个竖直排列的数表称为列. 元素 a_{ij} 处于第 i 行和第 j 列，称为 ij 表值. 通常将矩阵简记为 $A=[a_{ij}]$.

具有 m 个行和 n 个列的矩阵称为 m 乘 n 矩阵，记作 $m\times n$. 数偶 m 和 n 称为矩阵的型. 两个矩阵 A 与 B 称为相等的，记作 $A=B$，如果它们的行数和列数分别相等(同型)且对应元素相等. 于是，两个 $m\times n$ 矩阵相等等价于 mn 个等式组，其中每一等式都对应着一个元素偶.

只有一行的矩阵称为行矩阵或行向量，只行一列的矩阵称为列矩阵或列向量. 表值全部为零的矩阵称为零矩阵，记作 0.

例 5.4 (a) 矩形数表 $A=\begin{bmatrix} 1 & -4 & 5 \\ 0 & 3 & -2 \end{bmatrix}$为一个 2×3 矩阵. 其行为$[1,-4,5]$和$[0,3,-2]$，而列为$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -4 \\ 3 \end{bmatrix}, \begin{bmatrix} 5 \\ -2 \end{bmatrix}$.

(b) 2×4 的 0 矩阵为 $A=\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

(c) 设

$$\begin{bmatrix} x+y & 2z+t \\ x-y & z-t \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 5 \end{bmatrix}.$$

则其四个对应元素必定相等. 即

$$x+y=3, \quad x-y=1, \quad 2z+t=7, \quad z-t=5.$$

解上述方程组，得

$$x=2, \quad y=1, \quad z=4, \quad t=-1.$$

5.4 矩阵的加法和数乘

设 $A=[a_{ij}]$与 $B=[b_{ij}]$为两个 $m\times n$ 矩阵，即同型矩阵. A 与 B 的和记作 $A+B$，是将 A 与 B 的对应元素分别相加得到的矩阵. 即

$$A+B = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{bmatrix}.$$

数 k 与矩阵 A 的积，记作 $k\cdot A$ 或简记为 kA，是将数 k 乘以矩阵 A 的每一个元素得到的矩阵. 即

$$kA = \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ ka_{21} & ka_{22} & \cdots & ka_{2n} \\ \vdots & \vdots & & \vdots \\ ka_{m1} & ka_{m2} & \cdots & ka_{mn} \end{bmatrix}.$$

注意，$A+B$ 与 kA 仍然为 $m\times n$ 矩阵. 同样可以定义

$$-A = (-1)A, \qquad A-B = A+(-B).$$

矩阵$-A$称为矩阵A的负矩阵.不同型的矩阵的加法无定义.

例 5.5 设$A=\begin{bmatrix}1 & -2 & 3\\0 & 4 & 5\end{bmatrix}$,$B=\begin{bmatrix}4 & 6 & 8\\1 & -3 & -7\end{bmatrix}$.则

$$A+B=\begin{bmatrix}1+4 & -2+6 & 3+8\\0+1 & 4+(-3) & 5+(-7)\end{bmatrix}=\begin{bmatrix}5 & 4 & 9\\1 & 1 & -2\end{bmatrix}.$$

$$3A=\begin{bmatrix}3(1) & 3(-2) & 3(3)\\3(0) & 3(4) & 3(5)\end{bmatrix}=\begin{bmatrix}3 & -6 & 9\\0 & 12 & 15\end{bmatrix}.$$

$$2A-3B=\begin{bmatrix}2 & -4 & 6\\0 & 8 & 10\end{bmatrix}+\begin{bmatrix}-12 & -18 & -24\\-3 & 9 & 21\end{bmatrix}=\begin{bmatrix}-10 & -22 & -18\\-3 & 17 & 31\end{bmatrix}.$$

矩阵的加法和数乘运算具有下述性质.

定理 5.1 设A,B,C为同型矩阵,k,k'为数.则

(i) $(A+B)+C=A+(B+C)$.

(ii) $A+0=0+A$.

(iii) $A+(-A)=A-A=0$.

(iv) $A+B=B+A$.

(v) $k(A+B)=kA+kB$.

(vi) $(k+k')A=kA+k'A$.

(vii) $(kk')A=k(k'A)$.

(viii) $1A=A$.

注意,在(ii)和(iii)中,0表示零矩阵.由(i)和(iv),我们可以不加括号地作任意多个同型矩阵的和

$$A_1+A_2+\cdots+A_n.$$

这个和式与矩阵在其中的次序无关.进而,利用(vi)和(viii),我们有

$$A+A=2A,\quad A+A+A=3A,\quad \cdots.$$

由于具有n个分量的向量可以看做$1\times n$或$n\times 1$矩阵,所以定理5.1同样适用于向量的加法和数乘.

证明定理5.1只要对每个矩阵方程验证两边的第ij元素分别相等(见问题5.10).

5.5 矩阵的乘法

矩阵A与B的乘积,记作AB,稍稍有点复杂.我们首先从一个特例开始讨论.(这里用到的求和符号,大写希腊字母$\sum$的意义,可参考3.5.)

元素个数相同的行矩阵$A=[a_i]$与列矩阵$B=[b_i]$的积AB定义为

$$AB=[a_1,a_2,\cdots,a_n]\begin{bmatrix}b_1\\b_2\\\vdots\\b_n\end{bmatrix}=a_1b_1+a_2b_2+\cdots+a_nb_n=\sum_{k=1}^{n}a_kb_k.$$

即,AB是先将A与B的对应元素相乘然后把它们加起来的结果.注意AB是一个纯量(或为一个1×1矩阵).当A与B的元素个数不同时,AB无定义.

例 5.6 (a) $[7,-4,5]\begin{bmatrix}3\\2\\-1\end{bmatrix}=7(3)+(-4)(2)+5(3)=21-8-5=8.$

(b) $[6,-1,8,3]\begin{bmatrix}4\\-9\\-2\\5\end{bmatrix}=24+9-16+15=32.$

现在来讨论一般矩阵的乘法定义.

定义　设 $A=[a_{ik}]$和 $B=[b_{kj}]$为矩阵,满足 A 的列数等于 B 的行数. 即 A 为 $m\times p$ 矩阵而B 为 $p\times n$ 矩阵. 则 A 与 B 的乘积为一个 $m\times n$ 矩阵,其第 ij 元素为 A 的第 i 行乘以 B 的第 j 列的结果. 即

$$\begin{bmatrix} a_{11} & \cdots & a_{1p} \\ \cdot & & \cdot \\ a_{i1} & \cdots & a_{ip} \\ \cdot & & \cdot \\ a_{m1} & \cdots & a_{mp} \end{bmatrix}\begin{bmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1n} \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ b_{p1} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix}=\begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \cdot & \cdots & \cdot \\ \cdot & c_{ij} & \cdot \\ \cdot & \cdots & \cdot \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

其中

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{ip}b_{pj}=\sum_{k=1}^{p}a_{ik}b_{kj}.$$

我们强调,如果 $p\neq q$,则对于 $m\times p$ 矩阵A 与 $q\times n$ 矩阵 B,乘积 AB 无定义.

例 5.7　(a) 已知 $A=\begin{bmatrix}1 & 3\\ 2 & -1\end{bmatrix}$,$B=\begin{bmatrix}2 & 0 & -4\\ 5 & -2 & 6\end{bmatrix}$. 求 AB.

因为 A 为 2×2 矩阵而 B 为 2×3 矩阵,所以 AB 有定义且为 2×3 矩阵. 为求得乘积矩阵 AB 的第一行,以 A 的第一行[1,3]逐次乘以 B 的每一列

$$\begin{bmatrix}2\\5\end{bmatrix},\quad\begin{bmatrix}0\\-2\end{bmatrix},\quad\begin{bmatrix}-4\\6\end{bmatrix}.$$

即

$$AB=\begin{bmatrix}2+15 & 0-6 & -4+18\\ & & \end{bmatrix}=\begin{bmatrix}17 & -6 & 14\\ & & \end{bmatrix}.$$

为求得 AB 的第二行,以 A 的第二行[2,−1]逐次乘以 B 的每一列. 于是

$$AB=\begin{bmatrix}17 & -6 & 14\\ 4-5 & 0+2 & -8-6\end{bmatrix}=\begin{bmatrix}17 & -6 & 14\\ -1 & 2 & -14\end{bmatrix}.$$

(b) 设 $A=\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}$,$B=\begin{bmatrix}5 & 6\\ 0 & -2\end{bmatrix}$. 则

$$AB=\begin{bmatrix}5+0 & 6-4\\ 15+0 & 18-8\end{bmatrix}=\begin{bmatrix}5 & 2\\ 15 & 10\end{bmatrix}.$$

而

$$BA=\begin{bmatrix}5+18 & 10+24\\ 0-6 & 0-8\end{bmatrix}=\begin{bmatrix}23 & 34\\ -6 & -8\end{bmatrix}.$$

例 5.7(b)表明,矩阵的乘法不满足交换律,即矩阵的乘积 AB 与 BA 不相等. 矩阵的乘法满足下列运算规律.

定理 5.2　设 A,B,C 为矩阵. 并设以下乘法和加法均有定义.

(i) $(AB)C=A(BC)$　(结合律).

(ii) $A(B+C)=AB+AC$　(左分配律).

(iii) $(B+C)A=BA+CA$　(右分配律).

(iv) $k(AB)=(kA)B=A(kB)$　(其中 k 为数).

注意 $0A=0$, $B0=0$,其中 0 为零矩阵.

矩阵的乘法与线性方程组

任意一个线性方程组 S 等价于一个矩阵方程

$$AX = B.$$

其中 A 为方程组的系数构成的矩阵，X 为未知数构成的列向量，而 B 为常数项构成的列向量.(这里,等价意指方程组 S 的任一组解都是矩阵方程 $AX=B$ 的解,反之亦然.)例如,线性方程组

$$\begin{cases} x+2y-3z=4, \\ 5x-6y+8z=9 \end{cases}$$

等价于

$$\begin{bmatrix} 1 & 2 & -3 \\ 5 & -6 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 9 \end{bmatrix}.$$

容易看出,线性方程组可由下列矩阵

$$M = [A,B] = \begin{bmatrix} 1 & 2 & -3 & 4 \\ 5 & -6 & 8 & 9 \end{bmatrix}$$

完全确定,称此矩阵为线性方程组的增广矩阵.

5.6 转置矩阵

矩阵 A 的转置矩阵记作 A^T,是将 A 的行依次写作为列得到的矩阵. 例如

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}.$$

又如

$$[1, -3, -5]^T = \begin{bmatrix} 1 \\ -3 \\ -5 \end{bmatrix}.$$

注意,若 A 为一个 $m \times n$ 矩阵,则 A^T 为一个 $n \times m$ 矩阵. 特别地,行向量的转置为列向量,列向量的转置为行向量. 进而,若 $B=[b_{ij}]$为 $A=[a_{ij}]$的转置矩阵,则对所有的 i,j,有 $b_{ij}=a_{ji}$.

矩阵的转置运算满足下列性质.

定理 5.3 设 A,B 为矩阵,k 为值数. 并设下列加法和乘法均为可行.

(i) $(A+B)^T=A^T+B^T$.

(ii) $(kA)^T=kA^T$.

(iii) $(AB)^T=B^TA^T$.

(iv) $(A^T)^T=A$.

注意(iii),矩阵乘积的转置等于转置矩阵的乘积,但是乘积的次序逆转.

5.7 方　　阵

行数和列数相等的矩阵称为方阵. 具有 n 行 n 列的方阵称为 n 阶方阵,也叫做 n 方阵.

n 阶方阵 $A=[a_{ij}]$的主对角线或简称对角线由元素 $a_{11}, a_{22}, \cdots, a_{nn}$ 构成.

n 阶单位阵记作 I_n,或简记为 I,是主对角线元素均为 1、其余元素均为 0 的方阵. 单位阵在矩阵乘法中的角色恰如数 1 在通常数的乘法中的角色一样. 特别地,对任意方阵 A,有

$$AI = IA = A.$$

例如,考虑矩阵

$$\begin{bmatrix}1 & -2 & 0\\ 0 & -4 & -6\\ 5 & 3 & 2\end{bmatrix},\qquad \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}.$$

这两个矩阵都是方阵.但是第一个矩阵是3阶的,且对角线元素为1,−4,2.而第二个矩阵为4阶的,对角线元素全为1其余元素全为0,因此它是一个4阶单位阵.

方阵的代数运算

设 A 为任意方阵.我们可以作 A 与其自身的乘积.事实上,我们可以给出 A 的所有非负方幂如下:

$$A^2 = AA,\quad A^3 = A^2A,\quad \cdots\quad A^{n+1} = A^nA,\quad \cdots,\quad A^0 = I(A \neq 0).$$

同样可以定义矩阵 A 的多项式.特别地,对于任意多项式

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

其中 a_i 为数,我们定义 $f(A)$ 为下列矩阵

$$f(A) = a_0I + a_1A + a_2A^2 + \cdots + a_nA^n.$$

注意,我们是在 $f(x)$ 中以 A 代 x,以 a_0I 代 a_0 得到 $f(A)$ 的.当 $f(A)$ 为零矩阵时,A 称为多项式 $f(x)$ 的一个零点或根.

例 5.8　设 $A=\begin{bmatrix}1 & 2\\ 3 & -4\end{bmatrix}$.则

$$A^2 = \begin{bmatrix}1 & 2\\ 3 & -4\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & -4\end{bmatrix} = \begin{bmatrix}7 & -6\\ -9 & 22\end{bmatrix}.$$

$$A^3 = A^2A = \begin{bmatrix}7 & -6\\ -9 & 22\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & -4\end{bmatrix} = \begin{bmatrix}-11 & 38\\ 57 & -106\end{bmatrix}.$$

设 $f(x)=2x^2-3x+5$.则

$$f(A) = 2\begin{bmatrix}7 & -6\\ -9 & 22\end{bmatrix} - 3\begin{bmatrix}1 & 2\\ 3 & -4\end{bmatrix} + 5\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}16 & -18\\ -27 & 61\end{bmatrix}.$$

设 $g(x)=x^2+3x-10$.则

$$g(A) = \begin{bmatrix}7 & -6\\ -9 & 22\end{bmatrix} + 3\begin{bmatrix}1 & 2\\ 3 & -4\end{bmatrix} - 10\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}.$$

于是 A 为多项式 $g(x)$ 的一个根.

5.8　可逆(非奇异)矩阵和逆矩阵

方阵 A 称为可逆的或非奇异的,如果存在矩阵 B 满足

$$AB = BA = I.$$

这样的矩阵 B 必定是惟一存在的(问题 5.24),且称为 A 的逆阵,记作 A^{-1}.显然,B 是 A 的逆阵当且仅当 A 是 B 的逆阵.例如,假设

$$A = \begin{bmatrix}2 & 5\\ 1 & 3\end{bmatrix},\qquad B = \begin{bmatrix}3 & -5\\ -1 & 2\end{bmatrix}.$$

则

$$AB=\begin{bmatrix}6-5 & -10+10\\3-3 & -5+6\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},$$

而且

$$BA=\begin{bmatrix}6-5 & 15-15\\-2-2 & -5+6\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}.$$

于是 A 与 B 为互逆的.

例 5.9

$$\begin{bmatrix}1 & 0 & 2\\2 & -1 & 3\\4 & 1 & 8\end{bmatrix}\begin{bmatrix}-11 & 2 & 2\\-4 & 0 & 1\\6 & -1 & -1\end{bmatrix}$$

$$=\begin{bmatrix}-11+0+12 & 2+0-2 & 2+0-2\\-22+4+18 & 4+0-3 & 4-1-3\\-44-4+48 & 8+0-8 & 8+1-8\end{bmatrix}=\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}.$$

于是两个矩阵是互逆的,各自为对方的逆阵.

5.9 行列式

对于每个 n 阶方阵 A,我们分配一个特定的数与之对应,称为 A 的行列式,记作det(A)或 $|A|$,或

$$A=\begin{vmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\a_{21} & a_{22} & \cdots & a_{2n}\\\vdots & \vdots & & \vdots\\a_{n1} & a_{n2} & \cdots & a_{nn}\end{vmatrix}.$$

我们特别强调,用两条竖线括起来的一张正方形数表称为一个 n 阶行列式,它不是矩阵,但是它表示由行列式函数分配给一个方阵的数.

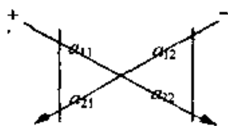
1,2,3 阶行列式的定义如下:

$$|a_{11}|=a_{11}.$$

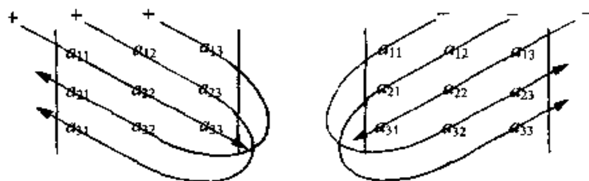
$$\begin{vmatrix}a_{11} & a_{12}\\a_{21} & a_{22}\end{vmatrix}=a_{11}a_{22}-a_{12}a_{21}.$$

$$\begin{vmatrix}a_{11} & a_{12} & a_{13}\\a_{21} & a_{22} & a_{23}\\a_{31} & a_{32} & a_{33}\end{vmatrix}=a_{11}a_{22}a_{33}+a_{12}a_{23}a_{31}+a_{13}a_{21}a_{32}-a_{13}a_{22}a_{31}-a_{12}a_{21}a_{33}-a_{11}a_{23}a_{32}.$$

下面的对角线法则可以帮助读者记忆 2 阶行列式.



也就是说,2 阶行列式等于沿着标以加号箭头的元素的积减去沿着标以减号箭头的元素的积. 类似的方法可以给出 3 阶行列式. 为清楚起见,我们将加号箭头和减号箭头分为两个图画出.



需要指出的是，对于高阶行列式，没有对角线法则.

例 5.10 (a) $\begin{vmatrix} 5 & 4 \\ 2 & 3 \end{vmatrix} = 5(3)-4(2)=15-8=7$,

$$\begin{vmatrix} 2 & 1 \\ -4 & 6 \end{vmatrix} = 2(6)-1(-4)=12+4=16.$$

(b) $$\begin{vmatrix} 2 & 1 & 3 \\ 4 & 6 & -1 \\ 5 & 1 & 0 \end{vmatrix} = 2(6)(0)+1(-1)(5)+3(1)(4)-3(6)(5)$$

$$-1(4)(0)-2(1)(-1)$$

$$=0-5+12-90-0+2$$

$$=-81.$$

行列式的一般定义

n 阶行列式的一般定义如下：

$$\det(A) = \sum \operatorname{sgn}(\sigma) a_{1j_1} a_{2j_2} \cdots a_{nj_n}.$$

其中求和对 $\{1,2,\cdots,n\}$ 的所有可能排列 $\sigma=\{j_1,j_2,\cdots,j_n\}$ 进行. 这里 $\operatorname{sgn}(\sigma)$ 等于 $+1$ 或 -1，分别对应于将 σ 变成自然次序时所需作的对换次数为偶数或奇数的情形. 我们已经完整地给出了行列式函数的一般定义. 对于阶数大于 3 的一般行列式的计算，读者可以参阅有关矩阵理论或线性代数书籍. 排列将在第六章中讨论.

行列式函数的一个重要性质是它的乘法. 即

定理 5.4 设 A,B 为任意的 n 阶方阵. 则

$$\det(AB) = \det(A) \times \det(B).$$

本定理的证明已超出本书的要求.

行列式与 2×2 矩阵的逆阵

设

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

为任意一个 2×2 矩阵. 我们来导出一个求 A 的逆阵 A^{-1} 的公式. 特别地，我们只要寻求 $2^2=4$ 个数 x_1,y_1,x_2,y_2，使得

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

或

$$\begin{bmatrix} ax_1+by_1 & ax_2+by_2 \\ cx_1+dy_1 & cx_2+dy_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

由上述矩阵相等，其对应元素相等，可以得到如下的 2×2 方程组：

$$\begin{cases} ax_1+by_1=1, \\ cx_1+dy_1=0; \end{cases} \qquad \begin{cases} ax_2+by_2=0, \\ cx_2+dy_2=1. \end{cases}$$

上述两个方程组的增广矩阵分别为：

$$\begin{bmatrix} a & b & 1 \\ c & d & 0 \end{bmatrix}, \quad \begin{bmatrix} a & b & 0 \\ c & d & 1 \end{bmatrix}.$$

(注意原矩阵 A 是这两个方程组的系数矩阵.)

假设 $|A| = ad - bc \neq 0$. 则上述方程组对 x_1, y_1, x_2, y_2 有惟一解,解为

$$x_1 = \frac{d}{ad-bc} = \frac{d}{|A|}, \quad y_1 = \frac{-c}{ad-bc} = \frac{-c}{|A|},$$

$$x_2 = \frac{-b}{ad-bc} = \frac{-b}{|A|}, \quad y_2 = \frac{a}{ad-bc} = \frac{a}{|A|}.$$

由此,

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix} = \frac{1}{|A|}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

用语言来描述,即:当 $|A| \neq 0$ 时,2×2 矩阵 A 的逆阵可以通过下述步骤求出:

(1) 调换主对角线上元素的位置.

(2) 在其余元素前加负号.

(3) 将结果矩阵乘以 $1/|A|$,即以 $|A|$ 除 A 中的每一个元素.

例如,若 $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$,则 $|A| = -2$. 因此,

$$A^{-1} = \frac{1}{-2}\begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -\frac{5}{2} & \frac{3}{2} \\ 2 & -1 \end{bmatrix}.$$

另一方面,若 $|A| = 0$,则不能解出未知数 x_1, y_1, x_2, y_2, A^{-1} 也就不存在. 对于高阶方阵,尽管没有更简单的公式来计算其逆,但这个性质对于一般情况也是成立的. 即有下列定理.

定理 5.5 方阵 A 可逆当且仅当其行列式非零.

5.10 初等行变换,高斯消去法

本节在初等行变换的基础上讨论高斯消去法.

初等行变换

我们将矩阵 $A = [a_{ij}]$ 的行依次记为 $R_1, R_2, \cdots, R_m$. 在行 R_i 中,第一个非零元素称为该行的首位非零元. 元素全部为零的行称为*零行*,于是零行没有首位非零元.

关于矩阵 A 的下列运算称为*初等行变换*.

[$\mathbf{E}_1$] 交换两行 R_i 与 R_j 的位置. 记作"交换 R_i 与 R_j".

[$\mathbf{E}_2$] 以非零数 k 乘以 R_i 行的每个元素. 记作"以 k 乘 R_i".

[$\mathbf{E}_3$] 将 R_i 行的倍数加到 R_j 行上,换句话说,就是以 $kR_i + R_j$ 替换 R_j,记作"R_j 加上 kR_i".

为避免步骤零散,我们可以将[$\mathbf{E}_2$]与[$\mathbf{E}_3$]合并为一步,即作下列变换:

[$\mathbf{E}$] 将 R_i 行的倍数加到 R_j 行的非零倍上,换句话说,即以 $kR_i + k'R_j$ 替换 R_j,其中 $k' \neq 0$.

注意,对于行变换[$\mathbf{E}_3$]和[$\mathbf{E}$],实际上只有 R_j 产生了变化.

记号 矩阵 A 与 B 称为*行等价*的,记作 $A \sim B$,如果矩阵 B 可以由矩阵 A 通过初等行变换得到.

阶梯矩阵

矩阵 A 称为*阶梯矩阵*或称为具有*阶梯形*,如果 A 满足下列两个条件:

(i) 所有的零行(如果存在)都排于矩阵的底部.

(ii) 每个非零元都排于该行首位非零元的右边.

矩阵称为具有行标准形,如果还满足下列性质:

(iii) 每个首位非零元均为 1.

(iv) 每个首位非零元为其所在列的惟一非零元.

零矩阵 0 为行标准形的一个特例. n 阶单位阵 I_n 是行标准形的另一个特例.

方阵 A 称为三角阵,如果其主对角线元素 $a_{11},a_{22},\cdots,a_{nn}$ 皆为首位非零元. 于是三角方阵为阶梯矩阵的特例. 单位阵为既是三角阵又是行标准形的惟一特例.

例 5.11 下列矩阵为阶梯矩阵,其中带圈的元素为首位非零元.

(在阶梯矩阵中,处于首位非零元之前和之下的零元素形成阶梯状,我们用阴影表示.)下述第三个矩阵为行标准形. 第二个矩阵不是行标准形,因为第三列包含了首位非零元之外的非零元. 第一个矩阵不是行标准形,因为有的首位非零元不是 1. 最后一个矩阵为三角阵.

$$\begin{bmatrix} \textcircled{2} & 3 & 2 & 0 & 4 & 5 & -6 \\ 0 & 0 & \textcircled{1} & 1 & -3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \textcircled{6} & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},\quad \begin{bmatrix} \textcircled{1} & 2 & 3 \\ 0 & 0 & \textcircled{1} \\ 0 & 0 & 0 \end{bmatrix},\quad \begin{bmatrix} 0 & \textcircled{1} & 3 & 0 & 0 & 4 \\ 0 & 0 & 0 & \textcircled{1} & 0 & -3 \\ 0 & 0 & 0 & 0 & \textcircled{1} & 2 \end{bmatrix},\quad \begin{bmatrix} \textcircled{2} & 4 & 7 \\ 0 & \textcircled{5} & 8 \\ 0 & 0 & \textcircled{6} \end{bmatrix}$$

矩阵格式的高斯消去法

设 A 为任意矩阵. 下面给出两个算法. 第一个算法将矩阵变为阶梯矩阵(只使用行初等变换),第二个算法将矩阵变为行标准形. 这两个算法合称高斯消去法.

算法 5.10A (向前消元) 输入任意矩阵 $A=[a_{ij}]$.

第一步 求出第一个具有非零元的列. 若这样的列不存在,则退出. (此时为零矩阵). 否则,设 j_1 表示该列的列号.

(a) 整理矩阵,使得 $a_{1j_1}\neq 0$. 即,若有必要,则交换行的次序,使得非零元出现于 j_1 列的第一行.

(b) 以 a_{1j_1} 为主元,将 a_{1j_1} 以下的元素变为零. 即,对于 $i>1$:

(1) 置 $m=-a_{ij_1}/a_{1j_1}$.

(2) 将 mR_1 加到 R_i 上.

[即以 $-(a_{ij_1}/a_{1j_1})R_1+R_i$ 替换 R_i.]

第二步 对于除第一行外的子矩阵,重复第一步. 这里,设 j_2 表示在子矩阵中具有非零元的第一个列. 因此,在第二步结束时,有 $a_{2j_2}\neq 0$.

第三步到第 $r+1$ 步 继续执行上述步骤,直到所得子矩阵没有非零元.

我们指出,在算法结束时,主元(首位非零元)将为

$$a_{1j_1},a_{2j_2},\cdots,a_{rj_r}.$$

其中 r 表示阶梯矩阵中非零行数.

注 1 在 1(b)步中,数字

$$m=-\frac{a_{i1}}{a_{11}}=-\frac{\text{将要消去的系数}}{\text{主元}}$$

称为乘数.

注 2 我们可以将 1(b)步改为

“将 $-a_{ij_1}R_1$ 加到 $a_{1j_1}R_i$ 上”

以避免分数的出现,使得元素的原有整数形式得以保持.

算法 5.10B（向后消元） 输入矩阵 $A=[a_{ij}]$为具有主元 $a_{1j_1},a_{2j_2},\cdots,a_{rj_r}$的阶梯阵.

第一步 (a) 以 $1/a_{rj_r}$乘以最后一个非零行R_r，使得该主元为 1.

(b) 从 $a_{rj_r}=1$ 出发将该主元以上元素变为零. 即，对于 $i=r-1,r-2,\cdots,1$：

(1) 置 $m=-a_{ir_r}$.

(2) 将 mR_r 加到R_i 上.

换言之，即利用初等行变换"将$-a_{ir_i}R_r$ 加到R_i 上".

[以$-a_{ir_i}R_r+R_i$ 替换R_i.]

第二步到第 $r-1$ 步 对于 R_{r-1}，R_{r-2}，…，R_2，重复第一步.

第 r 步 以 $1/a_{1j_1}$乘以 R_1.

例 5.12 求下列矩阵的标准形

$$\begin{bmatrix}1 & 2 & -3 & 1 & 2\\ 2 & 4 & -4 & 6 & 10\\ 3 & 6 & -6 & 9 & 13\end{bmatrix}.$$

首先利用算法 5.10A 将矩阵 A 化为阶梯矩阵. 特别地，以 $a_{11}=1$ 作为主元，将 a_{11} 以下的元素化为零. 即利用初等行变换"将$-2R_1$ 加到 R_2 上"和"将$-3R_1$ 加到 R_3 上". 然后，以 $a_{23}=2$ 作为主元将 a_{23}以下的元素化为零. 即作行变换"将$-\frac{3}{2}R_2$ 加到 R_3 上". 得到

$$A\sim\begin{bmatrix}1 & 2 & -3 & 1 & 2\\ 0 & 0 & 2 & 4 & 6\\ 0 & 0 & 3 & 6 & 7\end{bmatrix}\sim\begin{bmatrix}1 & 2 & -3 & 1 & 2\\ 0 & 0 & 2 & 4 & 6\\ 0 & 0 & 0 & 0 & -2\end{bmatrix}.$$

所给矩阵已经化为阶梯矩阵.

现在利用算法 5.10B 进一步将 A 化为行标准形. 特别地，以$-\frac{1}{2}$乘以 R_3，得到主元 $a_{35}=1$，然后利用 $a_{35}=1$ 将其上部元素化为零，即作行变换"将$-6R_3$ 加到 R_2 上"和"将$-2R_3$ 加到 R_1 上". 得到

$$A\sim\begin{bmatrix}1 & 2 & -3 & 1 & 2\\ 0 & 0 & 2 & 4 & 6\\ 0 & 0 & 0 & 0 & 1\end{bmatrix}\sim\begin{bmatrix}1 & 2 & -3 & 1 & 0\\ 0 & 0 & 2 & 4 & 0\\ 0 & 0 & 0 & 0 & 1\end{bmatrix}.$$

以$\frac{1}{2}$乘以 R_2 得主元 $a_{23}=1$，从 $a_{23}=1$ 出发，将其上部元素化为零. 即作行变换"将 $3R_2$ 加到 R_1 上". 得

$$A\sim\begin{bmatrix}1 & 2 & -3 & 1 & 0\\ 0 & 0 & 1 & 2 & 0\\ 0 & 0 & 0 & 0 & 1\end{bmatrix}\sim\begin{bmatrix}1 & 2 & 0 & 7 & 0\\ 0 & 0 & 1 & 2 & 0\\ 0 & 0 & 0 & 0 & 1\end{bmatrix}.$$

最后一个矩阵即为 A 的行标准形.

算法 5.10A 与 5.10B 表明，任一个矩阵必定行等价于至少一个行标准形矩阵. 实际上，在线性代数中，我们可以证明，这样的行标准形矩阵是惟一存在的. 即有下面的定理.

定理 5.6 任意矩阵 A 行等价于惟一一个行标准形矩阵（称为 A 的行标准形）.

线性方程组的矩阵解法

考虑线性方程组 S，或等价地，考虑以 $M=[A,B]$为增广矩阵的矩阵方程 $AX=B$. 我们可

以对矩阵 M 利用上述高斯消去法来解出这个线性方程组.

A 步(化简)　将增广矩阵 M 化为阶梯矩阵. 如果有一行具有形式 $(0,0,\cdots,0,b)$, $b\neq 0$, 则停止. 该方程组无解.

B 步(回代)　进一步将增广矩阵 M 化为其行标准形.

可以从 M 的标准形立即得到方程组的惟一解,或者当解不惟一时,得到解的自由变量表达式.

下例将上述算法应用于具有惟一解的方程组 S. 线性方程组无解或有无穷多解的情况分别见问题 5.32 和 5.31.

例 5.13　解线性方程组

$$\begin{cases} x+2y-z=3, \\ 2x+5y-z=-4, \\ 3x-2y-z=5. \end{cases}$$

将增广矩阵 M 化为阶梯矩阵进而化为行标准形.

$$M=\begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & 5 & -1 & -4 \\ 3 & -2 & -1 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & -8 & -4 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & -28 & -84 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix}.$$

于是,方程组的惟一解为 $x=2, y=-1, z=3$, 或等价地,写为向量形式 $u=(2,-1,3)$. 注意到,由 M 的阶梯矩阵为三角阵已经可以看出方程组具有惟一解.

$n\times n$ 矩阵的逆阵

考虑一个任意的 3×3 矩阵 $A=[a_{ij}]$. 则求 $A^{-1}=[x_{ij}]$ 的问题即为求解 3 个 3×3 线性方程组的问题. 这三个线性方程组的增广矩阵分别如下:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & 1 \\ a_{21} & a_{22} & a_{23} & 0 \\ a_{31} & a_{32} & a_{33} & 0 \end{bmatrix}, \quad \begin{bmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 1 \\ a_{31} & a_{32} & a_{33} & 0 \end{bmatrix}, \quad \begin{bmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 0 \\ a_{31} & a_{32} & a_{33} & 1 \end{bmatrix}.$$

注意,原矩阵 A 是所有三个线性方程组的系数矩阵,而且,三个方程组的常数项列构成一个单位阵 I. 这三个线性方程组可以由下列算法同时解出,此法适用于任何的 $n\times n$ 矩阵.

算法 5.10C　求任意 $n\times n$ 矩阵 A 的逆阵.

第一步　构造一个 $n\times 2n$ 矩阵 $M=[A,I]$, 即 M 的左边一半为 A 而右边一半为单位阵 I.

第二步　利用初等行变换将 M 化为阶梯阵. 如果在运算过程中在 M 的 A 部分出现零行,则停止(此时 A 没有逆阵). 否则, A 的部分将变为三角阵.

第三步　继续利用初等行变换将 M 化为行标准形

$$M\sim[I,B].$$

此时 M 的左边 A 的部分已经变为 I.

第四步　置 $A^{-1}=B$. 其中 B 即为 M 的行标准形中的右边一半.

例 5.14 求逆矩阵

$$A=\begin{bmatrix}1 & 0 & 2\\ 2 & -1 & 3\\ 4 & 1 & 8\end{bmatrix}.$$

作矩阵 $M=[A,I]$ 并化 M 为阶梯阵.

$$M=\left[\begin{array}{ccc|ccc}1 & 0 & 2 & 1 & 0 & 0\\ 2 & -1 & 3 & 0 & 1 & 0\\ 4 & 1 & 8 & 0 & 0 & 1\end{array}\right]$$

$$\sim\left[\begin{array}{ccc|ccc}1 & 0 & 2 & 1 & 0 & 0\\ 0 & -1 & -1 & -2 & 1 & 0\\ 0 & 1 & 0 & -4 & 0 & 1\end{array}\right]$$

$$\sim\left[\begin{array}{ccc|ccc}1 & 0 & 2 & 1 & 0 & 0\\ 0 & -1 & -1 & -2 & 1 & 0\\ 0 & 0 & -1 & -6 & 1 & 1\end{array}\right].$$

在 M 的阶梯阵中,其左边一半为三角阵,因此 A 可逆.进一步将 M 化为行标准形.

$$M\sim\left[\begin{array}{ccc|ccc}1 & 0 & 0 & -11 & 2 & 2\\ 0 & -1 & 0 & 4 & 0 & -1\\ 0 & 0 & 1 & 6 & -1 & -1\end{array}\right]$$

$$\sim\left[\begin{array}{ccc|ccc}1 & 0 & 0 & -11 & 2 & 2\\ 0 & 1 & 0 & -4 & 0 & 1\\ 0 & 0 & 1 & 6 & -1 & -1\end{array}\right].$$

最后的矩阵左边已化为单位阵,因此右边即为 A^{-1}. 于是

$$A^{-1}=\begin{bmatrix}-11 & 2 & 2\\ -4 & 0 & 1\\ 6 & -1 & -1\end{bmatrix}.$$

5.11 布尔(零-幺)矩阵

二进制数或二进制位为符号 0 和 1. 考虑这些数字的下列运算:

+	0	1
0	0	1
1	1	1

×	0	1
0	0	0
1	0	1

将二进制数看做逻辑值(0 表示 F, 1 表示 T),则上述运算分别对应于逻辑运算"或"(∨)以及"与"(∧). 即

∨	F	T
F	F	T
T	T	T

∧	F	T
F	F	F
T	F	T

(上述关于 0 和 1 的运算又称为布尔运算,因为它们同样对应于第十五章将要讨论的布尔代数运算.)

相对于上述的布尔运算,设矩阵 $A=[a_{ij}]$ 的元素为位元 0 或 1. 则 A 称为布尔矩阵. 两个布尔矩阵的布尔积除遵从通常矩阵乘法规则外,在数的运算中则采用布尔运算. 例如,设已知

$$A=\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix},\quad B=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}.$$

则

$$AB=\begin{bmatrix}0+0 & 1+1\\ 0+0 & 1+0\end{bmatrix}=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}.$$

可以证明，如果 A，B 为布尔矩阵，则布尔积 AB 为对 A 和 B 作通常矩阵乘积之后，将其中任何非零数替换为 1 即可.

问题与解答

向量

5.1 设 $u=(2,-7,1)$，$v=(-3,0,4)$，$w=(0,5,-8)$. 求

(a) $u+v$.　(b) $v+w$.　(c) $-3u$.　(d) $-w$.

解 ☞ (a) 将对应分量相加，得

$$u+v=(2,-7,1)+(-3,0,4)=(2-3,-7+0,1+4)=(-1,-7,5).$$

(b) 将对应分量相加，得

$$v+w=(-3,0,4)+(0,5,-8)=(-3+0,0+5,4-8)=(-3,5,-4).$$

(c) 将 u 的每个分量乘以 -3，得

$$-3u=-3(2,-7,1)=(-6,21,-3).$$

(d) 将 w 的每个分量反号，或等价地将每个分量乘以 -1，得

$$-w=-(0,5,-8)=(0,-5,8).$$

5.2 设 u，v，w 为问题 5.1 中的向量. 求：

(a) $3u-4v$.

(b) $2u+3v-5w$.

解 ☞ 首先进行向量的数乘，然后作向量的加法.

(a) $3u-4v=3(2,-1,7)-4(-3,0,4)=(6,-21,3)+(12,0,-16)=(18,-21,-13)$.

(b) $2u+3v-6w=2(2,-1,7)+3(-3,0,4)-5(0,5,-8)=(4,-14,2)+(-9,0,12)+(0,-25,40)=(-5,-39,54)$.

5.3 设 u，v，w 为问题 5.1 中的向量. 求：

(a) $u\cdot v$.　(b) $u\cdot w$.　(c) $v\cdot w$.

解 ☞ (a) $u\cdot v=2(-3)-7(0)+1(4)=-6+0+4=-2$.

(b) $u\cdot w=2(0)-7(5)+1(-8)=0-35-8=-43$.

(c) $v\cdot w=-3(0)+0(5)+4(-8)=0+0-32=-32$.

5.4 求 $\|u\|$. 其中 (a) $u=(3,-12,-4)$；　(b) $u=(2,-3,8,-7)$.

解 ☞ (a) $\|u\|^2=(3)^2+(-12)^2+(-4)^2=9+144+16=169$. $\|u\|=\sqrt{169}=13$.

(b) $\|u\|^2=4+9+64+49=126$，$\|u\|=\sqrt{126}=3\sqrt{14}$.

5.5 设 $x(1,1)+y(2,-1)=(1,4)$. 求 x，y.

解 ☞ 将 x，y 分别乘以向量后相加，得

$$x(1,1)+y(2,-1)=(x,x)+(2y,-y)=(x+2y,x-y)=(1,4).$$

因为两个向量相等仅当其对应分量相等，由此得到方程组

$$\begin{cases}x+2y=1,\\x-y=4.\end{cases}$$

解这个方程组得 $x=3$，$y=-1$.

5.6 设

$$u=\begin{bmatrix}5\\3\\-4\end{bmatrix},\quad v=\begin{bmatrix}-1\\5\\2\end{bmatrix},\quad w=\begin{bmatrix}3\\-1\\-2\end{bmatrix}.$$

求 (a) $5u-2v$　(b) $-2u+4v-3w$.

解 ☞　(a) $5u-2v=5\begin{bmatrix}5\\3\\-4\end{bmatrix}-2\begin{bmatrix}-1\\5\\2\end{bmatrix}=\begin{bmatrix}25\\15\\-20\end{bmatrix}+\begin{bmatrix}2\\-10\\4\end{bmatrix}=\begin{bmatrix}27\\5\\-24\end{bmatrix}$.

(b) $-2u+4v-3w=\begin{bmatrix}-10\\-6\\8\end{bmatrix}+\begin{bmatrix}-4\\20\\8\end{bmatrix}+\begin{bmatrix}-9\\3\\6\end{bmatrix}=\begin{bmatrix}-23\\17\\22\end{bmatrix}$.

矩阵的加法和数乘

5.7　给定

$$A=\begin{bmatrix}1 & 2 & -3\\4 & -5 & 6\end{bmatrix},\quad B=\begin{bmatrix}1 & -1 & 2\\0 & 3 & -5\end{bmatrix}.$$

求：(a) $A+B$　(b) $3A$ 与 $-4B$.

解 ☞　(a) 将对应元素分别相加，得

$$A+B=\begin{bmatrix}1+1 & 2+(-1) & -3+2\\4+0 & -5+3 & 6+(-5)\end{bmatrix}=\begin{bmatrix}2 & 1 & -1\\4 & -2 & 1\end{bmatrix}.$$

(b) 以给定的数乘以矩阵的每一个元素，得

$$3A=\begin{bmatrix}3(1) & 3(2) & 3(-3)\\3(4) & 3(-5) & 3(6)\end{bmatrix}=\begin{bmatrix}3 & 6 & -9\\12 & -15 & 18\end{bmatrix}.$$

$$-4B=\begin{bmatrix}-4(1) & -4(-1) & -4(2)\\-4(0) & -4(3) & -4(-5)\end{bmatrix}=\begin{bmatrix}-4 & 4 & -8\\0 & -12 & 20\end{bmatrix}.$$

5.8　已知

$$A=\begin{bmatrix}1 & -2 & 3\\4 & 5 & -6\end{bmatrix},\quad B=\begin{bmatrix}3 & 0 & 2\\-7 & 1 & 8\end{bmatrix}.$$

求：$2A-3B$.

解 ☞　首先作数乘矩阵，然后作矩阵的加法.

$$2A-3B=\begin{bmatrix}2 & -4 & 6\\8 & 10 & -12\end{bmatrix}+\begin{bmatrix}-9 & 0 & -6\\21 & -3 & -24\end{bmatrix}=\begin{bmatrix}-7 & -4 & 0\\29 & 7 & -36\end{bmatrix}.$$

(注意我们将 B 乘以 -3 然后相加，而不是乘以 3 然后相减. 这通常可以避免产生错误.)

5.9　已知

$$3\begin{bmatrix}x & y\\z & t\end{bmatrix}=\begin{bmatrix}x & 6\\-1 & 2t\end{bmatrix}+\begin{bmatrix}4 & x+y\\z+t & 3\end{bmatrix}.$$

求 x,y,z,t.

解 ☞　首先将两边写为一个矩阵，

$$\begin{bmatrix}3x & 3y\\3z & 3t\end{bmatrix}=\begin{bmatrix}x+4 & x+y+6\\z+t-1 & 2t+3\end{bmatrix}.$$

由两边对应元素相等，得到下列线性方程组

$$\begin{cases}3x=x+4,\\3y=x+y+6,\\3z=z+t-1,\\3t=2t+3,\end{cases}\quad 即\quad \begin{cases}2x=4,\\2y=6+x,\\2z=t-1,\\t=3,\end{cases}$$

得到方程组的解为 $x=2,y=4,z=1,t=3$.

5.10　证明定理 5.1(v)：$k(A+B)=kA+kB$.

证 ☞　设 $A=[a_{ij}]$，$B=[b_{ij}]$. 则 $A+B$ 的 ij 位置上的元素为 $a_{ij}+b_{ij}$. 因此 $k(a_{ij}+b_{ij})$ 为 $k(A+B)$ 的 ij 位置上的元素. 另一方面，kA 与 kB 的 ij 位置上的元素分别为 ka_{ij} 与 kb_{ij}. 于是 $ka_{ij}+kb_{ij}$ 为 $kA+kB$ 的 ij 位置上的元素. 但是，$k(a_{ij}+b_{ij})=ka_{ij}+kb_{ij}$. 于是 $k(A+B)$ 与 $kA+kB$ 的对应位置元素相等. 从而 $k(A+B)=kA+kB$.

矩阵的乘法

5.11 计算：(a) $[3,-2,5]\begin{bmatrix}6\\1\\-4\end{bmatrix}$.　　(b) $[2,-1,7,4]\begin{bmatrix}5\\-3\\-6\\9\end{bmatrix}$.

解 ☞　将对应元素相乘然后相加.

(a) $[3,-2,5]\begin{bmatrix}6\\1\\-4\end{bmatrix}=3(6)-2(1)+5(-4)=18-2-20=-4$.

(b) $[2,-1,7,4]\begin{bmatrix}5\\-3\\-6\\9\end{bmatrix}=10+3-42+36=7$.

5.12 设$(r\times s)$表示一个 $r\times s$ 矩阵. 判定下列矩阵乘法是否有定义，若是，请指出乘积矩阵的型.

(a) $(2\times3)(3\times4)$.　　(b) $(4\times1)(1\times2)$.　　(c) $(1\times2)(3\times1)$.

(d) $(5\times2)(2\times3)$.　　(e) $(4\times4)(3\times3)$.　　(f) $(2\times2)(2\times4)$.

解 ☞　如果内项两个数字相等，则乘积有定义，外项的两个数字即为乘积矩阵的型.

(a) 2×4.　　(b) 4×2.　　(c) 无定义.

(d) 5×3.　　(e) 无定义.　　(f) 2×4.

5.13 设

$$A=\begin{bmatrix}1&3\\2&-1\end{bmatrix},\quad B=\begin{bmatrix}2&0&-4\\3&-2&6\end{bmatrix}.$$

求：(a) AB　　(b) BA.

解 ☞　(a) 因为 A 为 2×2 矩阵，而 B 为 2×3 矩阵，所以乘积 AB 有定义且为一个 2×3 矩阵. 为求得 AB 的第一行，以 A 的第一行$[1,3]$依次乘以 B 的列$\begin{bmatrix}2\\3\end{bmatrix}$, $\begin{bmatrix}0\\-2\end{bmatrix}$, $\begin{bmatrix}-4\\6\end{bmatrix}$. 得到

$$\begin{bmatrix}1&3\\2&-1\end{bmatrix}\begin{bmatrix}2&0&-4\\3&-2&6\end{bmatrix}=\begin{bmatrix}1(2)+3(3)&1(0)+3(-1)&1(-4)+3(6)\\ & & \end{bmatrix}$$

$$=\begin{bmatrix}2+9&0-6&-4+18\\ & & \end{bmatrix}=\begin{bmatrix}11&-6&14\\ & & \end{bmatrix}.$$

为求出 AB 的第二行，以 A 的第二行$[2,-1]$依次乘以 B 的各列，得到

$$\begin{bmatrix}1&3\\2&-1\end{bmatrix}\begin{bmatrix}2&0&-4\\3&-2&6\end{bmatrix}=\begin{bmatrix}11&-6&14\\4-3&0+2&-8-6\end{bmatrix}.$$

于是

$$AB=\begin{bmatrix}11&-6&14\\1&2&-14\end{bmatrix}.$$

(b) 注意到 B 为 2×3 矩阵，而 A 为 2×2 矩阵，内项两个数字 3 与 2 不等，故乘积 BA 无定义.

5.14 计算：

(a) $\begin{bmatrix}1&6\\-3&5\end{bmatrix}\begin{bmatrix}4&0\\2&-1\end{bmatrix}$.

(b) $\begin{bmatrix}1&6\\-3&5\end{bmatrix}\begin{bmatrix}2\\-7\end{bmatrix}$.

(c) $\begin{bmatrix} 1 \\ -6 \end{bmatrix}\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}$.

(d) $\begin{bmatrix} 1 \\ -6 \end{bmatrix}[3,2]$.

(e) $[2,1]\begin{bmatrix} 1 \\ -6 \end{bmatrix}$.

解 ☞ (a) 第一矩阵为 2×2,第二矩阵为 2×2,因此乘积有定义且为 2×2 矩阵.

$$\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 2 & -1 \end{bmatrix}=\begin{bmatrix} 4+12 & 0+12 \\ -12+10 & 0-5 \end{bmatrix}=\begin{bmatrix} 16 & -6 \\ -2 & -5 \end{bmatrix}.$$

(b) 第一矩阵为 2×2 而第二矩阵为 2×1 矩阵,因此乘积有定义且为 2×1 矩阵.

$$\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 2 \\ -7 \end{bmatrix}=\begin{bmatrix} 2 & -42 \\ -6 & -35 \end{bmatrix}=\begin{bmatrix} -40 \\ -41 \end{bmatrix}.$$

(c) 第一矩阵为 2×1 矩阵,而第二矩阵为 2×2 矩阵. 两个内项 1 与 2 不等,乘积无定义.

(d) 第一矩阵为 2×1 矩阵,而第二矩阵为 1×2 矩阵,故乘积有定义且为 2×2 矩阵.

$$\begin{bmatrix} 1 \\ 6 \end{bmatrix}[3,2]=\begin{bmatrix} 1(3) & 1(2) \\ 6(3) & 6(2) \end{bmatrix}=\begin{bmatrix} 3 & 2 \\ 18 & 12 \end{bmatrix}.$$

(e) 第一矩阵为 1×2 矩阵,而第二矩阵为 2×1 矩阵,因此乘积有定义且为 1×1 矩阵,即为一个数.

$$[2,1]\begin{bmatrix} 1 \\ -6 \end{bmatrix}=2(1)-1(-6)=2+6=8.$$

5.15 证明定理 5.2(i): $(AB)C=A(BC)$.

证 ☞ 设 $A=[a_{ij}]$,$B=[b_{jk}]$,$C=[c_{kl}]$. 再设 $AB=S=[s_{ik}]$,$BC=T=[t_{jl}]$. 则

$$s_{ik}=a_{i1}b_{1k}+a_{i2}b_{2k}+\cdots+a_{im}b_{mk}=\sum_{j=1}^{m}a_{ij}b_{jk}.$$

$$t_{jl}=b_{j1}c_{1l}+b_{j2}c_{2l}+\cdots+b_{jn}c_{nl}=\sum_{k=1}^{n}b_{jk}c_{kl}.$$

现在将 S 与 C 相乘,即将(AB)与 C 相乘. 矩阵$(AB)C$ 的第 i 行,第 j 列的元素为

$$s_{i1}c_{1l}+s_{i2}c_{2l}+\cdots+s_{in}c_{nl}=\sum_{k=1}^{n}s_{ik}c_{kl}=\sum_{k=1}^{n}\sum_{j=1}^{m}(a_{ij}b_{jk})c_{kl}.$$

另一方面,我们将 A 与 T 即(BC)相乘,则矩阵 $A(BC)$的第 i 行,第 j 列的元素为

$$a_{i1}t_{1l}+a_{i2}t_{2l}+\cdots+a_{im}t_{ml}=\sum_{j=1}^{m}a_{ij}t_{jl}=\sum_{k=1}^{n}\sum_{j=1}^{m}a_{ij}(b_{jk}c_{kl}).$$

上述两个和式相等,定理得证.

转置矩阵

5.16 求下列矩阵的转置矩阵.

$$A=\begin{bmatrix} 1 & -2 & 3 \\ 7 & 8 & -9 \end{bmatrix},\quad B=\begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix},$$

$$C=[1,-3,5,-7],\quad D=\begin{bmatrix} 2 \\ -4 \\ 6 \end{bmatrix}.$$

解 ☞ 将矩阵的行写为对应的列,即可得其转置矩阵.

$$A^T=\begin{bmatrix} 1 & 7 \\ -2 & 8 \\ 3 & -9 \end{bmatrix},\quad B^T=\begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix},$$

$$C^T=\begin{bmatrix}1\\-3\\5\\-7\end{bmatrix},\quad D^T=[2,\ -4,6].$$

（注意，$B^T=B$，具有这种性质的矩阵称为对称矩阵. 同样，我们看到，行向量 C 的转置为一个列向量，而列向量 D 的转置为一个行向量.）

5.17　设

$$A=\begin{bmatrix}1&2&0\\3&-1&4\end{bmatrix}.$$

求：(a) AA^T.　　(b) A^TA.

解 ☞　首先将 A 的行写为对应列求得 $A^T=\begin{bmatrix}1&3\\2&-1\\0&4\end{bmatrix}$，然后，我们有

(a) $AA^T=\begin{bmatrix}1&-2&3\\7&8&-9\end{bmatrix}\begin{bmatrix}1&3\\2&-1\\0&4\end{bmatrix}=\begin{bmatrix}1+4+0&3-2+0\\3-2+0&9+1+16\end{bmatrix}=\begin{bmatrix}5&1\\1&26\end{bmatrix}.$

(b) $A^TA=\begin{bmatrix}1&3\\2&-1\\0&4\end{bmatrix}\begin{bmatrix}1&-2&3\\7&8&-9\end{bmatrix}=\begin{bmatrix}1+9&2-3&0+12\\2-3&4+1&0-4\\0-12&0-4&0+16\end{bmatrix}$

$=\begin{bmatrix}10&-1&12\\-1&5&-4\\12&-4&16\end{bmatrix}.$

5.18　证明定理 5.3(iii)：　$(AB)^T=B^TA^T$.

证 ☞　设 $A=[a_{ik}]$，$B=[b_{kj}]$. 则 AB 的 ij 元素为

$$a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{im}b_{mj}.\tag{1}$$

将(1)中每项交换次序，则(1)是$(AB)^T$ 的 ji 元素.

另一方面，B 的第 j 列变为 B^T 的第 j 行，而 A 的第 i 行变为 A^T 的第 j 列. 由此，B^TA^T 的 ji 元素为

$$[b_{1j},b_{2j},\cdots,b_{mj}]\begin{bmatrix}a_{i1}\\a_{i2}\\\vdots\\a_{im}\end{bmatrix}=b_{1j}a_{i1}+b_{2j}a_{i2}+\cdots+b_{mj}a_{im}.$$

于是，由对应元素相等得，$(AB)^T=B^TA^T$.

方阵

5.19　求下列矩阵的对角线元素.

(a) $A=\begin{bmatrix}1&3&6\\2&-5&8\\4&-2&7\end{bmatrix}$.

(b) $B=\begin{bmatrix}t-2&3\\-4&t+5\end{bmatrix}$.

(c) $C=\begin{bmatrix}1&2&-3\\4&-5&6\end{bmatrix}$.

解 ☞　(a) 对角线元素为矩阵中从左上角到右下角的元素构成. 即元素 a_{11},a_{22},a_{33}. 于是 A 的对角线元素为 $1,-5,7$.

(b) 对角线元素为有序偶$[t-2,t+5]$.

(c) 只有方阵才有对角线元素，而 C 不是方阵.

5.20　设

$$A=\begin{bmatrix}1 & 2\\4 & -3\end{bmatrix}.$$

求：(a) A^2.　　(b) A^3.

解 ☞　(a) $A^2=AA=\begin{bmatrix}1 & 2\\4 & -3\end{bmatrix}\begin{bmatrix}1 & 2\\4 & -3\end{bmatrix}=\begin{bmatrix}1+8 & 2-6\\4-12 & 8+9\end{bmatrix}=\begin{bmatrix}9 & -4\\-8 & 17\end{bmatrix}$.

(b) $A^3=AA^2=\begin{bmatrix}1 & 2\\4 & -3\end{bmatrix}\begin{bmatrix}9 & -4\\-8 & 17\end{bmatrix}=\begin{bmatrix}9-16 & -4+34\\36+24 & -16-51\end{bmatrix}=\begin{bmatrix}-7 & 30\\60 & -67\end{bmatrix}$.

5.21　设 $f(x)=2x^3-4x+5$，$g(x)=x^2+2x-11$. 对于问题 5.20 中的矩阵 A，求：

(a) $f(A)$.　　(b) $g(A)$.

解 ☞　(a) 为求 $f(A)$，首先在 $f(x)=2x^3-4x+5$ 中，将 A 代替 x 并以 $5I$ 代替常数项 5.

$$f(A)=2A^3-4A+5I=2\begin{bmatrix}-7 & 30\\60 & -67\end{bmatrix}-4\begin{bmatrix}1 & 2\\4 & -3\end{bmatrix}+5\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}.$$

然后计算每个数乘矩阵

$$f(A)=2A^3-4A+5I=\begin{bmatrix}-14 & 60\\120 & -134\end{bmatrix}+\begin{bmatrix}-4 & -8\\-16 & 12\end{bmatrix}+\begin{bmatrix}5 & 0\\0 & 5\end{bmatrix}.$$

最后将矩阵的对应元素相加，得

$$f(A)=\begin{bmatrix}-14-4+5 & 60-8+0\\120-16+0 & -134+12+5\end{bmatrix}=\begin{bmatrix}-13 & 52\\104 & -117\end{bmatrix}.$$

(b) 为求 $g(A)$，首先在 $g(x)=x^2+2x-11$ 中，将 A 代替 x 并以 $11I$ 代替常数项 11.

$$\begin{aligned}g(A)&=A^2+2A-11I\\&=\begin{bmatrix}9 & -4\\-8 & 17\end{bmatrix}+2\begin{bmatrix}1 & 2\\4 & -3\end{bmatrix}-11\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\\&=\begin{bmatrix}9 & -4\\-8 & 17\end{bmatrix}+\begin{bmatrix}2 & 4\\8 & -6\end{bmatrix}+\begin{bmatrix}-11 & 0\\0 & -11\end{bmatrix}\\&=\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}.\end{aligned}$$

(因为 $g(A)=0$，所以矩阵 A 为多项式 $g(x)$ 的一个根.)

行列式与逆矩阵

5.22　求下列矩阵的行列式.

(a) $\begin{bmatrix}4 & 5\\-3 & -2\end{bmatrix}$，　(b) $\begin{bmatrix}-2 & 7\\0 & 6\end{bmatrix}$，　(c) $\begin{bmatrix}a-b & b\\b & a+b\end{bmatrix}$，　(d) $\begin{bmatrix}a-b & a\\a & a+b\end{bmatrix}$.

解 ☞　利用公式 $\begin{vmatrix}a & b\\c & d\end{vmatrix}=ad-bc$ 计算.

(a) $\begin{vmatrix}4 & 5\\-3 & -2\end{vmatrix}=4(-2)-5(-3)=-8+15=7$.

(b) $\begin{vmatrix}-2 & 7\\0 & 6\end{vmatrix}=-2(6)-7(0)=-12+0=-12$.

(c) $\begin{vmatrix}a-b & b\\b & a+b\end{vmatrix}=(a-b)(a+b)-b^2=a^2-b^2-b^2=a^2-2b^2$.

(d) $\begin{vmatrix}a-b & a\\a & a+b\end{vmatrix}=(a-b)(a+b)-a^2=a^2-b^2-a^2=-b^2$.

5.23　求下列矩阵的行列式.

(a) $\begin{bmatrix}1 & 2 & 3\\4 & -2 & 3\\0 & 5 & -1\end{bmatrix}$.　　(b) $\begin{bmatrix}4 & -1 & -2\\0 & 2 & -3\\5 & 2 & 1\end{bmatrix}$.　　(c) $\begin{bmatrix}2 & -3 & 4\\1 & 2 & -3\\-1 & -2 & 5\end{bmatrix}$.

(提示：利用 5.9 的对角线法则).

解 (a) $\begin{vmatrix}1 & 2 & 3\\4 & -2 & 3\\0 & 5 & -1\end{vmatrix}=2+0+60-0-15+8=55.$

(b) $\begin{vmatrix}4 & -1 & -2\\0 & 2 & -3\\5 & 2 & 1\end{vmatrix}=8+15+0+20+24+0=67.$

(c) $\begin{vmatrix}2 & -3 & 4\\1 & 2 & -3\\-1 & -2 & 5\end{vmatrix}=20-9-8+8-12+15=14.$

5.24 如果存在,求下列矩阵的逆矩阵.

(a) $A=\begin{bmatrix}5 & 3\\4 & 2\end{bmatrix}$.　(b) $B=\begin{bmatrix}2 & -3\\1 & 3\end{bmatrix}$.　(c) $C=\begin{bmatrix}-2 & 6\\3 & -9\end{bmatrix}$.

解 因为所给均为 2×2 矩阵,所以可以利用 5.9 导出的公式.

(a) 首先求得$|A|=5(2)-3(4)=10-12=-2$. 然后,逆转对角线元素的次序,将非对角线元素取其相反数,并乘以 $1/|A|$,得

$$A^{-1}=-\frac{1}{2}\begin{bmatrix}2 & -3\\-4 & 5\end{bmatrix}=\begin{bmatrix}-1 & \frac{3}{2}\\2 & -\frac{5}{2}\end{bmatrix}.$$

(b) 首先求得$|B|=2(3)-(-3)(1)=6+3=9$. 然后,逆转对角线元素的次序,将非对角线元素取其相反数,并乘以 $1/|B|$,得

$$B^{-1}=\frac{1}{9}\begin{bmatrix}3 & 3\\-1 & 2\end{bmatrix}=\begin{bmatrix}\frac{1}{3} & \frac{1}{3}\\-\frac{1}{9} & \frac{2}{9}\end{bmatrix}.$$

(c) 首先求出$|C|=-2(-9)-6(3)=18-18=0$. 因为$|C|=0$,所以逆矩阵不存在.

5.25 已知

$$A=\begin{bmatrix}1 & -2 & 2\\2 & -3 & 6\\1 & 1 & 7\end{bmatrix}.$$

求 A 的逆矩阵.

解 构造矩阵 $M=[A,I]$,施以初等行变换,求出阶梯矩阵.

$$M=\left[\begin{array}{ccc|ccc}1 & -2 & 2 & 1 & 0 & 0\\2 & -3 & 6 & 0 & 1 & 0\\1 & 1 & 7 & 0 & 0 & 1\end{array}\right]\sim\left[\begin{array}{ccc|ccc}1 & -2 & 2 & 1 & 0 & 0\\0 & 1 & 2 & -2 & 1 & 0\\0 & 3 & 5 & -1 & 0 & 1\end{array}\right]$$

$$\sim\left[\begin{array}{ccc|ccc}1 & -2 & 2 & 1 & 0 & 0\\0 & 1 & 2 & -2 & 1 & 0\\0 & 0 & -1 & 5 & -3 & 1\end{array}\right].$$

在 M 的阶梯矩阵中,对应于 A 的左边一半为三角阵,所以 A^{-1} 存在. 进一步将 M 化为行标准形,得

$$M\sim\left[\begin{array}{ccc|ccc}1 & -2 & 0 & 11 & -6 & 2\\0 & 1 & 0 & 8 & -5 & 2\\0 & 0 & 1 & -5 & 3 & -1\end{array}\right]\sim\left[\begin{array}{ccc|ccc}1 & 0 & 0 & 27 & -16 & 6\\0 & 1 & 0 & 8 & -5 & 2\\0 & 0 & 1 & -5 & 3 & -1\end{array}\right].$$

最后的矩阵为$[I,A^{-1}]$,即右边一半为 A^{-1}. 于是

$$A^{-1}=\begin{bmatrix}27 & -16 & 6\\8 & -5 & 2\\-5 & 3 & -1\end{bmatrix}.$$

5.26 已知

$$B=\begin{bmatrix}1 & 3 & -4\\1 & 5 & -1\\3 & 13 & -6\end{bmatrix}.$$

求 B 的逆阵.

解 由矩阵 $M=[B,I]$ 出发,利用初等行变换化为阶梯矩阵.

$$M=\begin{bmatrix}1 & 3 & -4 & \vdots & 1 & 0 & 0\\ 1 & 5 & -1 & \vdots & 0 & 1 & 0\\ 3 & 13 & -6 & \vdots & 0 & 0 & 1\end{bmatrix}\sim\begin{bmatrix}1 & 3 & -4 & \vdots & 1 & 0 & 0\\ 0 & 2 & 3 & \vdots & -1 & 1 & 0\\ 0 & 4 & 6 & \vdots & -3 & 0 & 1\end{bmatrix}$$

$$\sim\begin{bmatrix}1 & 3 & -4 & \vdots & 1 & 0 & 0\\ 0 & 2 & 3 & \vdots & -1 & 1 & 0\\ 3 & 0 & 0 & \vdots & -1 & -2 & 1\end{bmatrix}.$$

在 M 的阶梯矩阵中,左边一半具有零行,即 B 不能化为三角阵.因此 B 没有逆矩阵.

5.27 设 A 为可逆阵,且 B 为其逆矩阵.换言之,$AB=BA=I$.证明逆矩阵 B 是惟一存在的.

证 设 B_1,B_2 为 A 的任意两个逆矩阵.即

$$AB_1=B_1A=I,\qquad AB_2=B_2A=I.$$

则 $B_1=B_1I=B_1(AB_2)=(B_1A)B_2=IB_2=B_2$.

5.28 设 A,B 为同阶可逆阵.证明 AB 可逆,且 $(AB)^{-1}=B^{-1}A^{-1}$.

证 我们有

$$(AB)(B^{-1}A^{-1})=A(BB^{-1})A^{-1}=AIA^{-1}=AA^{-1}=I,$$

而且

$$(B^{-1}A^{-1})(AB)=B^{-1}(A^{-1}A)B=B^{-1}IB=B^{-1}B=I.$$

所以,$B^{-1}A^{-1}$ 为 AB 的逆矩阵,即 $(AB)^{-1}=B^{-1}A^{-1}$.

阶梯矩阵,初等行变换,高斯消去法

5.29 交换下列矩阵的行的次序,以获得阶梯矩阵.

(a) $\begin{bmatrix}0 & 1 & -3 & 4 & 6\\ 4 & 0 & 2 & 5 & -3\\ 0 & 0 & 7 & -2 & 8\end{bmatrix}$; (b) $\begin{bmatrix}0 & 0 & 0 & 0 & 0\\ 1 & 2 & 3 & 4 & 5\\ 0 & 0 & 5 & -4 & 7\end{bmatrix}$;

(c) $\begin{bmatrix}0 & 2 & 2 & 2 & 2\\ 0 & 3 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0\end{bmatrix}$.

解 (a) 交换第一,第二行的位置.

(b) 将零行换到最后一行.

(c) 不需要作任何变换,矩阵已为阶梯矩阵.

5.30 对下列矩阵进行初等行变换,使之变为阶梯矩阵.

$$A=\begin{bmatrix}1 & 2 & -3 & 0\\ 2 & 4 & -2 & 2\\ 3 & 6 & -4 & 3\end{bmatrix}.$$

解 以 a_{11} 为主元,将 a_{11} 下面的元素化为零.即利用行变换"将 $-2R_1$ 加到 R_2 上"以及"将 $-3R_1$ 加到 R_3 上".得到

$$\begin{bmatrix}1 & 2 & -3 & 0\\ 0 & 0 & 4 & 2\\ 0 & 0 & 5 & 3\end{bmatrix}.$$

以 $a_{23}=4$ 作为主元,将 a_{23} 下面的元素化为零.即利用初等行变换"将 $-5R_2$ 加到 $4R_3$ 上",得到

$$\begin{bmatrix}1 & 2 & -3 & 0\\ 0 & 0 & 4 & 2\\ 0 & 0 & 0 & 2\end{bmatrix}.$$

最后的矩阵即为阶梯矩阵.

5.31 下列阶梯矩阵中,何者为行标准形?

$$\begin{bmatrix}1 & 2 & -3 & 0 & 1\\0 & 0 & 5 & 2 & -4\\0 & 0 & 0 & 7 & 3\end{bmatrix},\quad \begin{bmatrix}0 & 1 & 7 & -5 & 0\\0 & 0 & 0 & 0 & 1\\0 & 0 & 0 & 0 & 0\end{bmatrix},\quad \begin{bmatrix}1 & 0 & 5 & 0 & 2\\0 & 1 & 2 & 0 & 4\\0 & 0 & 0 & 1 & 7\end{bmatrix}.$$

解 ☞　第一个矩阵不是行标准形,因为有两个首非零元分别为 5 和 7 而不是 1,而且,在首非零元 5 和 7 的上面还有非零元. 第二和第三个矩阵都是行标准形.

5.32　将下列矩阵化为行标准形.

$$A=\begin{bmatrix}1 & -2 & 3 & 1 & 2\\1 & 1 & 4 & -1 & 3\\2 & 5 & 9 & -2 & 8\end{bmatrix}.$$

解 ☞　首先,通过"将 $-R_1$ 加到 R_2 上","将 $-2R_1$ 加到 R_3 上"以及"将 $-3R_2$ 加到 R_3 上"这一系列行初等变换将 A 化为阶梯矩阵.

$$A\sim\begin{bmatrix}1 & -2 & 3 & 1 & 2\\0 & 3 & 1 & -2 & 1\\0 & 9 & 3 & -4 & 4\end{bmatrix}\sim\begin{bmatrix}1 & -2 & 3 & 1 & 2\\0 & 3 & 1 & -2 & 1\\0 & 0 & 0 & 2 & 1\end{bmatrix}.$$

现在,利用回代过程将上述阶梯矩阵化为 A 的行标准形. 首先将 R_3 乘以 $\frac{1}{2}$ 以获得主元 $a_{34}=1$,再通过"将 $2R_3$ 加到 R_2 上","将 $-R_3$ 加到 R_1 上",得到

$$A\sim\begin{bmatrix}1 & -2 & 3 & 1 & 2\\0 & 3 & 1 & -2 & 1\\0 & 0 & 0 & 1 & \frac{1}{2}\end{bmatrix}\sim\begin{bmatrix}1 & -2 & 3 & 0 & \frac{3}{2}\\0 & 3 & 1 & 0 & 2\\0 & 0 & 0 & 1 & \frac{1}{2}\end{bmatrix}.$$

将 R_2 乘以 $\frac{1}{3}$ 得到主元 $a_{22}=1$,并利用行变换"将 $2R_2$ 加到 R_1 上"得到

$$A\sim\begin{bmatrix}1 & -2 & 3 & 0 & \frac{3}{2}\\0 & 1 & \frac{1}{3} & 0 & \frac{2}{3}\\0 & 0 & 0 & 1 & \frac{1}{2}\end{bmatrix}\sim\begin{bmatrix}1 & 0 & \frac{11}{3} & 0 & \frac{17}{6}\\0 & 1 & \frac{1}{3} & 0 & \frac{2}{3}\\0 & 0 & 0 & 1 & \frac{1}{2}\end{bmatrix}.$$

因为 $a_{11}=1$,所以最后的矩阵为 A 的行标准形.

5.33　利用增广矩阵 M 解下列线性方程组.

$$\begin{cases}x+3y-2z+t=3,\\2x+6y-5z-3t=7.\end{cases}$$

解 ☞　将增广矩阵 M 化为阶梯矩阵,进而化为行标准形.

$$M=\begin{bmatrix}1 & 3 & -2 & 1 & 3\\2 & 6 & -5 & -3 & 7\end{bmatrix}\sim\begin{bmatrix}1 & 3 & -2 & 1 & 3\\0 & 0 & 1 & -5 & 1\end{bmatrix}\sim\begin{bmatrix}1 & 3 & 0 & -9 & 5\\0 & 0 & 1 & -5 & 1\end{bmatrix}.$$

对应于行标准形,重新写出线性方程组如下:

$$\begin{cases}x+3y-9t=5,\\z-5t=1.\end{cases}$$

在两个方程中首先出现的未知数 x,z 称为基本变量,其余未知数 y 和 t 称为自由变量. 将自由变量移到各方程的右边,得到解的自由变量表达式

$$\begin{cases}x=5-3y+9t,\\z=1+5t.\end{cases}$$

我们可以令自由变量 y 和 t 分别取参数值如 $y=a,t=b$ 以获得方程组的解的参数形式. 即

$$x=5-3a+9b,\quad y=a,\quad z=1+5b,\quad t=b.$$

或表示为向量形式

$$u=(5-3a+9b,a,1+5b,b).$$

我们可以给参数任意赋值，并从中解出基本变量而得到方程组的一个特定参数解. 例如，令 $y=2,t=3$，得 $x=26,z=16$. 于是

$$x=26,\quad y=2,\quad z=16,\quad t=3$$

或

$$u=(26,2,16,3)$$

为方程组的一个特定参数解.

5.34 利用增广矩阵 M 解下列线性方程组.

$$\begin{cases}x+y-2z+4t=5,\\2x+2y-3z+t=4,\\3x+3y-4z-2t=3.\end{cases}$$

解☞ 先将增广矩阵 M 化为阶梯矩阵，再化为行标准形.

$$M=\begin{bmatrix}1&1&-2&4&5\\2&2&-3&1&4\\3&3&-4&-2&3\end{bmatrix}\sim\begin{bmatrix}1&1&-2&4&5\\0&0&1&-7&-6\\0&0&2&-14&-12\end{bmatrix}\sim\begin{bmatrix}1&1&0&-10&-7\\0&0&1&-7&-6\end{bmatrix}.$$

（因为第二个矩阵的第三行与第二行成比例，从而将产生零行，所以我们将该矩阵中的第三行删去.）

对应于 M 的行标准形，重新写出线性方程组，然后将自由变量移到右边，获得解的自由变量表达式

$$\begin{cases}x+y-10t=-7,\\z-7t=-6.\end{cases}$$

从此，有

$$\begin{cases}x=-7-y+10t,\\z=-6+7t.\end{cases}$$

其中，x,z 为基本变量，而 y,t 为自由变量.

5.35 利用增广矩阵 M 解下列线性方程组.

$$\begin{cases}x-2y+4z=2,\\2x-3y+5z=3,\\3x-4y+6z=7.\end{cases}$$

解☞ 先将增广矩阵 M 化为阶梯矩阵.

$$M=\begin{bmatrix}1&-2&4&2\\2&-3&5&3\\3&-4&6&7\end{bmatrix}\sim\begin{bmatrix}1&-2&4&2\\0&1&-3&-1\\0&2&-6&1\end{bmatrix}\sim\begin{bmatrix}1&-2&4&2\\0&1&-3&-1\\0&0&0&3\end{bmatrix}.$$

在阶梯矩阵中，第三行对应于退化方程

$$0x+0y+0z=3.$$

于是原方程组无解.（注意，从阶梯矩阵可以看出原方程组是否有解.）

杂题

5.36 设

$$A=\begin{bmatrix}1&0&0\\0&0&1\\1&1&0\end{bmatrix},\qquad B=\begin{bmatrix}0&1&1\\1&0&0\\0&1&0\end{bmatrix}$$

为布尔矩阵. 求布尔积 AB，BA 和 A^2.

解☞ 先按通常方法求矩阵的积，然后将其中非零元全部替换为 1. 于是

$$AB=\begin{bmatrix}0&1&1\\0&1&0\\1&1&1\end{bmatrix},\quad BA=\begin{bmatrix}1&1&1\\1&0&0\\0&0&1\end{bmatrix},\quad A^2=\begin{bmatrix}1&0&0\\1&1&0\\1&0&1\end{bmatrix}.$$

5.37 设

$$A=\begin{bmatrix}1 & 3\\4 & -3\end{bmatrix}.$$

(a) 求非零列向量 $u=\begin{bmatrix}x\\y\end{bmatrix}$，使得 $Au=3u$.

(b) 表示出所有满足条件的向量.

解 (a) 首先写出矩阵方程，然后将两边写为单个矩阵(列向量).

$$A=\begin{bmatrix}1 & 3\\4 & -3\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}=3\begin{bmatrix}x\\y\end{bmatrix},$$

即 $\begin{bmatrix}x+3y\\4x-3y\end{bmatrix}=\begin{bmatrix}3x\\3y\end{bmatrix}$.

由两边对应元素相等可得线性方程组，将此方程组化为阶梯式.

$$\begin{cases}x+3y=3x\\4x-3y=3y\end{cases}，或\begin{cases}2x-3y=0\\4x-6y=0\end{cases}，或\begin{cases}2x-3y=0\\0=0\end{cases}，或\ 2x-3y=0.$$

方程组化为关于两个未知数的一个(非退化)方程. 因此有无穷多解. 为得到方程组的非零解，可令 $y=2$，则有 $x=3$. 于是 $u=[3,2]^T$ 为一个满足条件的向量.

(b) 为获得方程组的一般解，可令 $y=a$，其中 a 为一个参数. 对应于 $y=a$ 由方程 $2x-3y=0$ 得到 $x=3a/2$. 于是，$u=[3a/2,a]^T$ 表示所有满足条件的向量.

补　充　题

向量

5.38 设 $u=(1,-2,4)$，$v=(3,5,1)$，$w=(2,1,-3)$. 求：

(a) $3u-2v$.　(b) $4u-v-3w$.　(c) $5u+7v-2w$.

5.39 对于 5.38 中的已知向量，求：

(a) $u\cdot v, u\cdot w, v\cdot w$.　(b) $\|u\|, \|v\|, \|w\|$.

5.40 设 $u=(2,-1,0,-3)$，$v=(1,-1,-1,3)$，$w=(1,3,-2,2)$. 求：

(a) $2u-3v$.　(b) $5u-3v-4w$.　(c) $-u+2v-2w$.

(d) $u\cdot v, u\cdot w, v\cdot w$.　(e) $\|u\|, \|v\|, \|w\|$.

5.41 设

$$u=\begin{bmatrix}1\\3\\-4\end{bmatrix},\quad v=\begin{bmatrix}2\\1\\5\end{bmatrix},\quad w=\begin{bmatrix}3\\-2\\6\end{bmatrix}.$$

求：(a) $5u-3v$，　(b) $2u+4v-6w$，

(c) $u\cdot v, u\cdot w, v\cdot w$.　(d) $\|u\|, \|v\|, \|w\|$.

5.42 对于下列已知条件，分别求出 x，y.

(a) $x(2,5)+y(4,-3)=(8,33)$.　(b) $x(1,4)+y(2,-5)=(7,2)$.

5.43 已知

$$x\begin{bmatrix}1\\2\\3\end{bmatrix}+y\begin{bmatrix}2\\5\\-1\end{bmatrix}+z\begin{bmatrix}4\\-2\\3\end{bmatrix}=\begin{bmatrix}9\\-3\\16\end{bmatrix}.$$

求 x,y,z.

矩阵的运算

在问题 5.44 到 5.48 中，设已知下列矩阵

$$A=\begin{bmatrix}1 & 2\\3 & -4\end{bmatrix},\quad B=\begin{bmatrix}5 & 0\\-6 & 7\end{bmatrix},\quad C=\begin{bmatrix}1 & -3 & 4\\2 & 6 & -5\end{bmatrix},\quad D=\begin{bmatrix}3 & 7 & -1\\4 & -8 & 9\end{bmatrix}.$$

5.44 求：(a) $5A-2B$　(b) $C+D$　(c) $2C-3D$.

5.45 求：(a) AB (b) BA.

5.46 求：(a) AC (b) AD (c) BC (d) BD.

5.47 求：(a) A^T (b) C^T (c) C^TC (d) CC^T.

5.48 求：(a) $A^2=AA$ (b) $B^2=BB$ (c) $C^2=CC$.

在问题 5.49 至 5.52 中，设已知矩阵

$$A=\begin{bmatrix}1 & -1 & 2\\ 0 & 3 & 4\end{bmatrix},\quad B=\begin{bmatrix}4 & 0 & 3\\ -1 & -2 & 3\end{bmatrix},\quad C=\begin{bmatrix}2 & -3 & 0 & 1\\ 5 & -1 & -4 & 2\\ -1 & 0 & 0 & 3\end{bmatrix},\quad D=\begin{bmatrix}2\\ -1\\ 3\end{bmatrix}.$$

5.49 求：(a) $A+B$ (b) $A+C$ (c) $3A-4B$.

5.50 求：(a) AB (b) AC (c) AD.

5.51 求：(a) BC (b) BD (c) CD.

5.52 求：(a) A^T (b) A^TB (c) A^TC.

5.53 设 $A=\begin{bmatrix}1 & 2\\ 3 & 6\end{bmatrix}$. 求一个 2×2 的非零矩阵 B，使得 $AB=0$.

方阵

5.54 求下列矩阵的对角线元素.

$$\text{(a)}\begin{bmatrix}2 & -7 & 8\\ 3 & -6 & -5\\ 4 & 0 & -1\end{bmatrix},\quad \text{(b)}\begin{bmatrix}1 & 2 & -9\\ 3 & 1 & 8\\ 5 & -6 & -1\end{bmatrix},\quad \text{(c)}\begin{bmatrix}3 & 4 & -8\\ 2 & -7 & 0\end{bmatrix}.$$

5.55 设 $A=\begin{bmatrix}2 & -5\\ 3 & 1\end{bmatrix}$. 求：

(a) A^2 与 A^3.

(b) $f(A)$，其中 $f(x)=x^3-2x^2-5$.

(c) $g(A)$，其中 $g(x)=x^2-3x+17$.

5.56 设 $B=\begin{bmatrix}4 & -2\\ 1 & -6\end{bmatrix}$. 求：

(a) B^2 与 B^3.

(b) $f(B)$，其中 $f(x)=x^2+2x-22$.

(c) $g(B)$，其中 $g(x)=x^2-3x-6$.

5.57 设 $A=\begin{bmatrix}6 & -4\\ 3 & -2\end{bmatrix}$. 求一个非零列向量 $u=\begin{bmatrix}x\\ y\end{bmatrix}$ 使得 $Au=4u$.

行列式与逆矩阵

5.58 计算下列矩阵的行列式.

$$\text{(a)}\begin{bmatrix}2 & 5\\ 4 & 1\end{bmatrix}.\quad \text{(b)}\begin{bmatrix}6 & 1\\ 3 & -2\end{bmatrix}.\quad \text{(c)}\begin{bmatrix}4 & -5\\ 0 & 2\end{bmatrix}.\quad \text{(d)}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.\quad \text{(e)}\begin{bmatrix}-2 & 8\\ -5 & -2\end{bmatrix}.$$

5.59 计算下列矩阵的行列式.

$$\text{(a)}\begin{bmatrix}2 & 1 & 1\\ 0 & 5 & -2\\ 1 & -3 & 4\end{bmatrix}.\quad \text{(b)}\begin{bmatrix}3 & -2 & -4\\ 2 & 5 & -1\\ 0 & 6 & 1\end{bmatrix}.\quad \text{(c)}\begin{bmatrix}-2 & -1 & 4\\ 6 & -3 & -2\\ 4 & 1 & 2\end{bmatrix}.\quad \text{(d)}\begin{bmatrix}7 & 6 & 5\\ 1 & 2 & 1\\ 3 & -2 & 1\end{bmatrix}.$$

5.60 (如果存在)求下列矩阵的逆矩阵.

$$A=\begin{bmatrix}7 & 4\\ 5 & 3\end{bmatrix},\quad B=\begin{bmatrix}2 & 3\\ 4 & 5\end{bmatrix},\quad C=\begin{bmatrix}4 & -6\\ -2 & 3\end{bmatrix},\quad D=\begin{bmatrix}5 & -2\\ 6 & -3\end{bmatrix}.$$

5.61 (如果存在)求下列矩阵的逆矩阵.

$$A=\begin{bmatrix}1 & 2 & -4\\ -1 & -1 & 5\\ 2 & 7 & -3\end{bmatrix},\quad B=\begin{bmatrix}1 & -1 & 1\\ 0 & 2 & -2\\ 1 & 3 & -1\end{bmatrix},\quad C=\begin{bmatrix}1 & 2 & 3\\ 2 & 5 & -1\\ 5 & 12 & 1\end{bmatrix}.$$

阶梯矩阵，初等行变换和高斯消去法

5.62　对于下列各题，先将 A 化为阶梯矩阵，再化为行标准形。

(a) $A=\begin{bmatrix}1&2&-1&2&1\\2&4&1&-2&3\\3&6&2&-6&5\end{bmatrix}$.　(b) $A=\begin{bmatrix}2&3&-2&5&1\\3&-1&2&0&4\\4&-5&6&-5&7\end{bmatrix}$.

5.63　仅用 0 和 1，列出所有可能的 2×2 的阶梯矩阵.

5.64　仅用 0 和 1，求所有可能的 3×3 矩阵的行标准形的个数.

5.65　利用增广矩阵 M，解下列线性方程组：

(a) $\begin{cases}x+2y-4z=-3,\\2x+6y-5z=2,\\3x+11y-4z=12.\end{cases}$　(b) $\begin{cases}x+2y-4z=3,\\2x+6y-5z=10,\\3x+10y-6z=14.\end{cases}$

5.66　利用增广矩阵 M，解下列线性方程组.

(a) $\begin{cases}x-3y+2z-t=2,\\3x-9y+7z-t=7,\\2x-6y+7z+4t=7.\end{cases}$　(b) $\begin{cases}x+2y+3z=7,\\x+3y+z=6,\\2x+6y+5z=15,\\3x+10y+7z=23.\end{cases}$

杂题

5.67　设 $A=\begin{bmatrix}1&2\\0&1\end{bmatrix}$. 求 A^n.

5.68　对于矩阵 A,B，如果有 $AB=BA$，则称 A 与 B 为可交换的. 求所有与矩阵 $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ 可交换的矩阵 $\begin{bmatrix}x&y\\z&t\end{bmatrix}$.

5.69　设 $A=\begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix}$ 及 $B=\begin{bmatrix}1&0&0\\1&0&0\\0&1&1\end{bmatrix}$ 为布尔矩阵. 求下列布尔矩阵.

(a) $A+B$.　(b) AB.　(c) BA.　(d) A^2.　(e) B^2.

补充题答案

5.38　(a) $(-3,-16,10)$. (b) $(-5,-16,24)$. (c) $(22,23,33)$.

5.39　(a) $-3,-12,8$. (b) $\sqrt{21},\sqrt{35},\sqrt{14}$.

5.40　(a) $(1,1,3,-15)$. (b) $(3,-14,11,-32)$. (c) $(-2,-7,2,5)$. (d) $-6,-7,6$. (e) $\sqrt{14},\sqrt{12}=2\sqrt{3},\sqrt{18}=3\sqrt{2}$.

5.41　(a) $(-1,12,-35)^T$. (b) $(-8,22,-24)^T$. (c) $-15,-27,34$. (d) $\sqrt{26},\sqrt{30},7$.

5.42　(a) $x=2,y=-1$. (b) $x=3,y=2$.

5.43　$x=3,y=-1,z=2$.

5.44　(a) $\begin{bmatrix}-5&10\\27&-34\end{bmatrix}$.　(b) $\begin{bmatrix}4&4&3\\6&-2&4\end{bmatrix}$.　(c) $\begin{bmatrix}-7&-27&11\\-8&36&-37\end{bmatrix}$.

5.45　$AB=\begin{bmatrix}-7&14\\39&-28\end{bmatrix}$,　$BA=\begin{bmatrix}5&10\\15&-40\end{bmatrix}$.

5.46　$AC=\begin{bmatrix}5&9&-6\\-5&33&32\end{bmatrix}$,　$AD=\begin{bmatrix}11&-9&17\\-7&53&-39\end{bmatrix}$,　$BC=\begin{bmatrix}5&-15&20\\8&60&-59\end{bmatrix}$.

$BD=\begin{bmatrix}15&35&-5\\10&-98&69\end{bmatrix}$.

5.47 $A^T=\begin{bmatrix}1 & 3\\ 2 & -4\end{bmatrix}$， $C^T=\begin{bmatrix}1 & 2\\ -3 & 6\\ 4 & -5\end{bmatrix}$.

$C^TC=\begin{bmatrix}5 & 9 & -6\\ 9 & 45 & -42\\ -6 & -42 & 41\end{bmatrix}$， $CC^T=\begin{bmatrix}26 & -36\\ -36 & 65\end{bmatrix}$.

5.48 $A^2=\begin{bmatrix}7 & -6\\ -9 & 22\end{bmatrix}$， $B^2=\begin{bmatrix}25 & 0\\ -72 & 49\end{bmatrix}$. C^2 无定义.

5.49 (a) $\begin{bmatrix}5 & -1 & -1\\ -1 & 1 & 7\end{bmatrix}$.　(b) 无定义.　(c) $\begin{bmatrix}-13 & -3 & 18\\ 4 & 17 & 0\end{bmatrix}$.

5.50 AB 无定义.　$AC=\begin{bmatrix}-5 & -22 & 4 & 5\\ 11 & -3 & -12 & 18\end{bmatrix}$， $AD=\begin{bmatrix}9\\ 9\end{bmatrix}$.

5.51 $BC=\begin{bmatrix}11 & -12 & 0 & -5\\ -15 & 5 & 8 & 4\end{bmatrix}$， $BD=\begin{bmatrix}11\\ 9\end{bmatrix}$， CD 无定义.

5.52 $A^T=\begin{bmatrix}1 & 0\\ -1 & 3\\ 2 & 4\end{bmatrix}$， $A^TB=\begin{bmatrix}4 & 0 & -3\\ -7 & -6 & 12\\ 4 & -8 & 6\end{bmatrix}$， A^TC 无定义.

5.53 $B=\begin{bmatrix}2 & 4\\ -1 & -2\end{bmatrix}$.

5.54 (a) $[2,-6,-1]$.　(b) $[1,1,-1]$.　(c) 无定义.

5.55 $A^2=\begin{bmatrix}-11 & -15\\ 9 & -14\end{bmatrix}$.　$A^3=\begin{bmatrix}-67 & 40\\ -24 & -59\end{bmatrix}$.　$f(A)=\begin{bmatrix}-50 & 70\\ -42 & -36\end{bmatrix}$.　$g(A)=0$.

5.56 $B^2=\begin{bmatrix}14 & 4\\ -2 & 34\end{bmatrix}$， $B^3=\begin{bmatrix}60 & -52\\ 26 & -200\end{bmatrix}$， $f(B)=0$， $g(B)=\begin{bmatrix}-4 & 10\\ -5 & 46\end{bmatrix}$.

5.57 $u=(2a,a)^T$，a 为任意非零数.

5.58 (a) -18.　(b) -15.　(c) 8.　(d) 1.　(e) 44.

5.59 (a) 21.　(b) -11.　(c) 100.　(d) 0.

5.60 $A^{-1}=\begin{bmatrix}3 & -4\\ -5 & 7\end{bmatrix}$，$B^{-1}=\begin{bmatrix}-\frac{5}{2} & \frac{3}{2}\\ 2 & -1\end{bmatrix}$，$C^{-1}$ 无定义，$D^{-1}=\begin{bmatrix}1 & -\frac{2}{3}\\ 2 & -\frac{5}{3}\end{bmatrix}$.

5.61 $A^{-1}=\begin{bmatrix}-16 & -11 & 3\\ \frac{7}{2} & \frac{5}{2} & -\frac{1}{2}\\ -\frac{5}{2} & -\frac{3}{2} & \frac{1}{2}\end{bmatrix}$， $B^{-1}=\begin{bmatrix}1 & \frac{1}{2} & 0\\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2}\\ -\frac{1}{2} & -1 & \frac{1}{2}\end{bmatrix}$.　C^{-1} 无定义.

5.62 (a) $\begin{bmatrix}1 & 2 & -1 & 2 & 1\\ 0 & 0 & 3 & -6 & 1\\ 0 & 0 & 0 & -6 & 1\end{bmatrix}$， $\begin{bmatrix}1 & 2 & 0 & 0 & \frac{4}{3}\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & -\frac{1}{6}\end{bmatrix}$.

(b) $\begin{bmatrix}2 & 3 & -2 & 5 & 1\\ 0 & -11 & 10 & -15 & 5\\ 0 & 0 & 0 & 0 & 0\end{bmatrix}$， $\begin{bmatrix}1 & 0 & \frac{4}{11} & \frac{5}{11} & \frac{13}{11}\\ 0 & 1 & -\frac{10}{11} & \frac{15}{11} & -\frac{5}{11}\\ 0 & 0 & 0 & 0 & 0\end{bmatrix}$.

5.63 $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$， $\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}$， $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$， $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$， $\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$.

5.64 13 个.

5.65 (a) $x=3,y=1,z=2$.　(b) 无解.

5.66 (a) $x=3y-5t,y=1-2t$.　(b) $x=2,y=1,z=1$.

5.67 $A^n=\begin{bmatrix}1 & 2n\\0 & 1\end{bmatrix}$.

5.68 $\begin{bmatrix}a & b\\0 & a\end{bmatrix}$.

5.69 $A+B=\begin{bmatrix}1 & 1 & 0\\1 & 0 & 1\\1 & 1 & 1\end{bmatrix}$, $AB=\begin{bmatrix}1 & 0 & 0\\1 & 1 & 1\\1 & 0 & 0\end{bmatrix}$, $BA=\begin{bmatrix}0 & 1 & 0\\0 & 1 & 0\\1 & 0 & 1\end{bmatrix}$, $A^2=\begin{bmatrix}1 & 0 & 1\\1 & 1 & 0\\0 & 1 & 0\end{bmatrix}$, $B^2=\begin{bmatrix}1 & 0 & 0\\1 & 0 & 0\\1 & 0 & 0\end{bmatrix}$.

第六章 计 数

6.1 引言，基本计数原理

组合分析，包括排列、组合与划分的研究，涉及到确定某种事件的逻辑可能性的数目，而不必指出每一种情形. 本章采用两种基本计数原理.

加法原理 假设事件 E 能以 m 种方式出现，事件 F 能以 n 种方式出现，且两种事件不能同时出现. 那么 E 或 F 能以 $m+n$ 种方式出现. 更一般地，假设事件 E_1 能以 n_1 种方式出现，事件 E_2 能以 n_2 种方式出现，事件 E_3 能以 n_3 种方式出现，…，且任意两个事件不能同时出现. 那么事件 $E_1, E_2, E_3, \cdots$ 之一以 $n_1+n_2+n_3+\cdots$ 种方式出现.

例 6.1 (a) 假设教计算课的男教授有 8 名，女教授有 5 名. 那么同学可以有 $8+5=13$ 种方式选择计算课教授.

(b) 假设事件 E 为取一个小于 10 的素数，事件 F 为取一个小于 10 的偶数. 那么 E 有 4 种方式[2,3,5,7]，F 有 4 种方式[2,4,6,8]. 但 E 或 F 不能有 $4+4=8$ 种方式，因为 2 既是小于 10 的素数，也是小于 10 的偶数. 事实上，E 或 F 仅有 $4+4-1$ 种方式.

(c) 假设事件 E 为在 10 与 20 之间取一个素数，事件 F 为在 10 与 20 之间取一个偶数. 那么 E 有 4 种方式[11,13,17,19]，F 有 4 种方式[12,14,16,18]，于是 E 或 F 有 $4+4=8$ 种方式，因为，此时没有偶数为素数.

乘法原理 假设事件 E 有 m 种方式发生，独立于事件 E 之外的事件 F 有 n 种方式发生. 那么 E 和 F 的组合有 mn 种方式发生. 一般地，假设事件 E_1 有 n_1 种方式发生；随着 E_1，事件 E_2 有 n_2 种方式发生；随着 E_2、事件 E_3 有 n_3 种方式发生，等等. 那么，所有事件依照指定的顺序有 $n_1 \cdot n_2 \cdot n_3 \cdots$、种方式发生.

例 6.2 (a) 假设汽车牌照由两个字母，紧跟着 3 个数字组成，且第一个数字不为 0，问可以印制多少个不同的牌照？

每个字母有 26 种不同的选择，第一个数字有 9 种选择，另两个数字都有 10 种选择. 因此可印制

$$26 \cdot 26 \cdot 9 \cdot 10 \cdot 10 = 608\,400$$

种不同的牌照.

(b) 设有一个 26 人的组织，问有多少种方式选举一个主席，一个会计和一个秘书（假设没有人可担任两个职务）？

主席可以有 26 种选举方式. 接着，会计可以有 25 种选举方式（因为被选为主席的人不能做会计），再接着，秘书有 24 种选举方式. 于是，由上面的计数原理，该组织有

$$26 \cdot 25 \cdot 24 = 15\,600$$

种方式选举公务员.

上面两个计数原理有一个集合论解释. 特别地，用 $n(A)$ 表示集合 A 中元素的个数. 那么

(1) **加法原理** 若 A 与 B 不相交，则

$$n(A \cup B) = n(A) + n(B)$$

(2) **乘法原理** 设 $A \times B$ 为集合 A 与 B 的笛卡儿积，则

$$n(A \times B) = n(A) \cdot n(B).$$

6.2 阶乘符号

从 1 到 n（包括 1 和 n）的正整数的积记作 $n!$（读作 n 的阶乘）：

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdots (n-2)(n-1)n.$$

换句话说，$n!$ 可如此定义

$$1! = 1, \quad 且\ n! = n \cdot (n-1)!$$

为方便，定义 $0! = 1$.

例 6.3 (a) $2! = 1 \cdot 2 = 2$, $3! = 1 \cdot 2 \cdot 3 = 6$, $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$,

$5! = 5 \cdot 4! = 5 \cdot 24 = 120$, $6! = 6 \cdot 5! = 6 \cdot 120 = 720$.

(b) $\frac{8!}{6!} = \frac{8 \cdot 7 \cdot 6!}{6!} = 8 \cdot 7 = 56$, $12 \cdot 11 \cdot 10 = \frac{12 \cdot 11 \cdot 10 \cdot 9!}{9!} = \frac{12!}{9!}$,

$\frac{12 \cdot 11 \cdot 10}{1 \cdot 2 \cdot 3} = 12 \cdot 11 \cdot 10 \cdot \frac{1}{3!} = \frac{12!}{3!\ 9!}$.

(c) $$n(n-1)\cdots(n-r+1) = \frac{n(n-1)\cdots(n-r+1)(n-r)(n-r-1)\cdots 3 \cdot 2 \cdot 1}{(n-r)(n-r-1)\cdots 3 \cdot 2 \cdot 1} = \frac{n!}{(n-r)!}.$$

$$\frac{n(n-1)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdots (r-1)r} = n(n-1)\cdots(n-r+1) \cdot \frac{1}{r!} = \frac{n!}{(n-r)!} \cdot \frac{1}{r!} = \frac{n!}{r!\ (n-r)!}.$$

6.3 二项式系数

设 r 和 n 为正整数，$r \leqslant n$. 符号 $\binom{n}{r}$（读作“nCr”）定义为

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdots (r-1)r}.$$

由例 6.3(c)可以看出

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot (r-1)r} = \frac{n!}{r!(n-r)!}.$$

而 $n-(n-r)=r$，因此，有下面的重要关系：

$$\binom{n}{n-r} = \binom{n}{r}.$$

或，换句话说，若 $a+b=n$，则 $\binom{n}{a} = \binom{n}{b}$.

例 6.4 (a) $\binom{8}{2} = \frac{8 \cdot 7}{1 \cdot 2} = 28$, $\binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126$, $\binom{12}{5} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 792$,

$\binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = 120$, $\binom{13}{1} = \frac{13}{1} = 13$.

注意到 $\binom{n}{r}$ 的分子、分母都恰有 r 个因子.

(b) 计算 $\binom{10}{7}$. 由定义

$$\binom{10}{7} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7} = 120.$$

另一方面，$10-7=3$，因此，也可如下计算 $\binom{10}{7}$：

$$\binom{10}{7}=\binom{10}{3}=\frac{10\cdot 9\cdot 8}{1\cdot 2\cdot 3}=120.$$

注意,第二种方法省时省力.

二项式系数与 Pascal 三角形

$\binom{n}{r}$称为二项式系数,因为它们作为$(a+b)^n$ 的展开式的系数出现.特别地,可以证明

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

$a+b$ 的相继幂的系数可以排成三角形的数表,称为 Pascal 三角形,如图 6-1. Pascal 三角形中的数有如下交互性质:

(1) 每一行的第一个数与最后一个数都是 1.

(2) 数表中的每个其他数可通过相加位于其上方的两数得到.如,$10=4+6$,$15=5+10$,$20=10+10$.

$$(a+b)^0=1$$
$$(a+b)^1=a+b$$
$$(a+b)^2=a^2+2ab+b^2$$
$$(a+b)^3=a^3+3a^2b+3ab^2+b^3$$
$$(a+b)^4=a^4+4a^3b+6a^2b^2+4ab^3+b^4$$
$$(a+b)^5=a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$
$$(a+b)^6=a^6+6a^5b+15a^4b^2+20a^3b^3+15a^2b^4+6ab^5+b^6$$

………

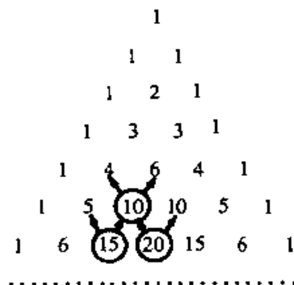


图 6-1　Pascal 三角形

由于 Pascal 三角形中的数都是二项式系数,所以,Pascal 三角形的性质(2)由下面的定理得到(在问题 6.7 中证明):

定理 6.1　$$\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}.$$

6.4 排　列

n 个对象以给定次序的任一安排称为这些对象(同时取出全部)的排列. n 个对象中的任 r 个对象以给定序的任一安排称为 r-排列,或称为 n 个对象取 r 个对象的排列.例如,考虑字母 a,b,c 和 d 的集合.则

(i) $bdca$,$dcba$ 与 $acdb$ 是 4 个字母的排列(同时取出全部);

(ii) bad,adb,cbd 与 bca 是 4 个字母取 3 个的排列;

(iii) ad,cb,da 与 bd 是 4 个字母取 2 个的排列.

n 个对象取 r 个的排列数记为

$$P(n,r),\quad nPr,\quad P_{n,r},\quad P_r^n,\quad 或(n)_r.$$

我们采用 $P(n,r)$.在得到 $P(n,r)$的一般公式前,我们考虑一个特殊情形.

例 6.5　求 6 个对象 A,B,C,D,E,F 取 3 个对象的排列数.即,求只用给定的 6 个字母,且不许重复的 3 个字母"单词"的个数.

用下面的 3 个方框表示一般的 3 个字母的"单词":

□ □ □

第一个字母有 6 种不同的选取方式,接着,第二个字母有 5 种不同的选取方式,最后,最后的字母有 4 种不同的选取方式.在适当的方框中如下写上每一个数:

6　5　4

于是,由基本计数原理,6 个字母的不许重复的 3 字母单词有 $6 \cdot 5 \cdot 4 = 120$ 种可能,即 6 个对象取 3 个对象的排列有 120 个.

$$P(6,3) = 120.$$

$P(n,r)$公式的推导

n 个对象取 r 个对象的排列数公式的推导,即 n 个对象的 r-排列数 $P(n,r)$ 的推导,遵循上面例子的过程. n 个对象的 r-排列中的第 1 个元素有 n 种选取方式,接着,排列中的第 2 个元素有 $n-1$ 种选取方式,再接着,排列中的第 3 个元素有 $n-2$ 种选取方式,继续下去,在 r-排列中的第 r 个(最后一个)对象有 $n-(r-1)=n-r+1$ 种选取方式. 于是,由基本计数原理,有

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1).$$

由例 6.3(c)可以看出

$$\begin{aligned} & n(n-1)(n-2)\cdots(n-r+1) \\ = & \frac{n(n-1)(n-2)\cdots(n-r+1)\cdot(n-r)!}{(n-r)!} = \frac{n!}{(n-r)!}. \end{aligned}$$

由此证明了下面的定理

定理 6.2　$P(n,r)=\dfrac{n!}{(n-r)!}$.

在 $r=n$ 的特殊情形中,我们有

$$P(n,n) = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 = n!.$$

因此,我们有如下推论.

推论 6.3　n 个对象(同时全取)的排列数为 $n!$

例如,3 个字母 a,b,c 的排列有 $3! = 3\cdot 2\cdot 1 = 6$ 个. 它们是 $abc, acb, bac, bca, cab, cba$.

可重排列

通常我们想知道可重集的排列数,可重集是指有某些元素相同的集合. 用

$$P(n;n_1,n_2,\cdots,n_r)$$

表示 n 个对象的排列数. 其中 n_1 个对象是相同的,n_2 个对象是相同的,…,n_r 个对象是相同的. 下面给出一般公式:

定理 6.4　$P(n;n_1,n_2,\cdots,n_r)=\dfrac{n!}{n_1!\ n_2!\ \cdots n_r!}$.

用一个特别的例子说明上面定理的证明. 假设我们想用单词"BABBY"中的字母构造所有可能的 5 字母"单词",对象 B_1, A_1, B_2, B_3, Y 的排列有 $5! = 120$ 个. 这里 B_1, B_2, B_3 是可区分的. 注意,去掉下标后,下面 6 个排列

$$B_1B_2B_3AY,\ B_2B_1B_3AY,\ B_3B_1B_2AY,\ B_1B_3B_2AY,\ B_2B_3B_1AY,\ B_3B_2B_1AY,$$

给出同样的单词. 6 源于这个事实:在排列的前 3 个位置放 B_1, B_2, B_3 有 $3! = 3\cdot 2\cdot 1 = 6$ 种不同的方法. 这对于任 3 个位置放 B_1, B_2, B_3 都是对的. 因此,利用单词"BABBY"的字母构造的 5 字母单词有

$$P(5;3) = \frac{5!}{3!} = \frac{120}{6} = 20.$$

例 6.6　(a) 用单词"BENZENE"的字母可以构成多少个 7 字母单词? 我们求 7 个对象的排列数,其中有 3 个相同的 E,两个相同的 N. 由定理 6.4,这样的单词数为

$$P(7;3,2) = \frac{7!}{3!2!} = \frac{7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{3\cdot 2\cdot 1\cdot 2\cdot 1} = 420.$$

(b) 用 4 面不可区分的红旗,3 面不可区分的白旗和一面蓝旗可以组成多少种不同的

信号？每个信号由 8 面垂直悬挂的旗子构成. 我们求 8 个对象的排列数，其中有 4 个对象是相同的，另有 3 个对象也是相同的. 这样的信号数为

$$P(8;4,3)=\frac{8!}{4!3!}=\frac{8\cdot7\cdot6\cdot5\cdot4\cdot3\cdot2\cdot1}{4\cdot3\cdot2\cdot1\cdot3\cdot2\cdot1}=280.$$

6.5 组　合

设有含 n 个对象的集合. n 个对象取 r 个对象的组合是 r 个对象的不计次序的任一选取. 换句话说，n 个对象的任一个 r-元素子集是一个 r-组合. 例如，字母 a,b,c,d 取 3 个元素的组合为

$$\{a,b,c\},\quad \{a,b,d\},\quad \{a,c,d\},\quad \{b,c,d\}$$

或简单地，abc,abd,acd,bcd. 注意下面的组合是相等的.

$$abc,acb,bac,bca,cab,cba$$

即，每个都表示同样的集合$\{a,b,c\}$.

n 个对象取 r 个的组合数记为 $C(n,r)$，在不同的课本中也会记为${}_nC_r$，$C_{n,r}$，C_n^r. 在给出 $C(n,r)$的一般公式之前，我们先考虑一个特殊情形.

例 6.7　求 4 个对象 a,b,c,d 取 3 个的组合数.

每个由 3 个物体构成的组合确定 3！=6 个该组合中对象的排列，如图6－2. 于是，组合数乘以 3！就等于排列数；即

$$C(4,3)\cdot3!=P(4,3)\quad 或\quad C(4,3)=\frac{P(4,3)}{3!}.$$

而 $P(4,3)=4\cdot3\cdot2=24$，$3!=6$. 由此，$C(4,3)=4$，见图 6－2.

组合	排列
abc	abc，acb，bac，bca，cab，cba
abd	abd，adb，bad，bda，dab，dba
acd	acd，adc，cad，cda，dac，dca
bcd	bcd，bdc，cbd，cdb，dbc，dcb

图 6－2

$C(n,r)$的公式

由于 n 个对象取 r 个的任一组合确定了该组合中对象的 $r!$ 个排列. 因此，有

$$P(n,r)=r!C(n,r).$$

于是得到

定理 6.5　$C(n,r)=\dfrac{P(n,r)}{r!}=\dfrac{n!}{r!\,(n-r)!}$.

回忆二项式系数$\binom{n}{r}$定义为$\dfrac{n!}{r!\,(n-r)!}$；因此

$$C(n,r)=\binom{n}{r}.$$

我们将交互地使用 $C(n,r)$和$\binom{n}{r}$.

例 6.8　(a) 8 人中可产生多少个 3 人委员会？

实际上，每个委员会就是 8 人取 3 人的一个组合. 于是可产生的委员会的数目为

$$C(8,3)=\binom{8}{3}=\frac{8\cdot7\cdot6}{1\cdot2\cdot3}=56.$$

(b) 一农民从拥有 6 头牛,5 头猪和 8 只鸡的某人处购买 3 头牛,2 头猪和 4 只鸡.问这个农民有多少种选择?

这个农民有$\binom{6}{3}$种方式选择牛,有$\binom{5}{2}$种方式选择猪,有$\binom{8}{4}$种方式选择鸡.因此,他选择这些动物共有

$$\binom{6}{3}\binom{5}{2}\binom{8}{4}=\frac{6\cdot5\cdot4}{1\cdot2\cdot3}\cdot\frac{5\cdot4}{1\cdot2}\cdot\frac{8\cdot7\cdot6\cdot5}{1\cdot2\cdot3\cdot4}=20\cdot10\cdot70=14000$$

种方式.

6.6 鸽笼原理

从下面近乎明显的叙述可以得到组合论的许多结果.

鸽笼原理 若 n 个鸽笼被 $n+1$ 只或更多只鸽子占据,则至少有一个鸽笼被超过一只鸽子占据.

这个原理可以应用于要证明某种情况必然发生的许多问题.

例 6.9 (a) 设一个系有 13 位教授,则必有两位教授(鸽子)在同一个月份(鸽笼)出生.

(b) 设一个洗衣袋中装有许多红色,白色和蓝色袜子,则只要取出 4 只袜子(鸽子)就一定有一双同色的(鸽笼)袜子.

(c) 至少要从集合 $S=\{1,2,3,\cdots,9\}$ 中取出几个元素就能保证有两数相加为 10?

这里 5 个集合$\{1,9\}$,$\{2,8\}$,$\{3,7\}$,$\{4,6\}$,$\{5\}$为鸽笼.这样任取 S 的 6 个元素(鸽子)就能保证有两个数相加为 10.

鸽笼原理有如下推广.

推广的鸽笼原理 若 n 个鸽笼被 $kn+1$ 只或更多只鸽子占据,k 为正整数,则至少有一个鸽笼被 $k+1$ 只或更多只鸽子占据.

例 6.10 (a) 在一个班的同学中至少取几名同学就能保证有 3 人在同一个月份出生?

这里 $n=12$ 个月份是鸽笼,而 $k+1=3$,即 $k=2$.因此,在任意 $kn+1=25$ 个同学(鸽子)中,有 3 人在同一个月份出生.

(b) 设洗衣袋中有许多红色,白色和蓝色袜子.至少取出多少只袜子就能保证同色的两双(4 只)袜子?

这里有 $n=3$ 种颜色(鸽笼),且 $k+1=4$,即 $k=3$.于是,在任意 $kn+1=10$ 只袜子(鸽子)中,有 4 只是同色的.

6.7 容斥原理

设 A,B 为两个有限集,则

$$n(A\cup B)=n(A)+n(B)-n(A\cap B).$$

换句话说,为了求并集 $A\cup B$ 中元素的个数 $n(A\cup B)$,先将 $n(A)$ 与 $n(B)$ 相加,再减去 $n(A\cap B)$;即"包含"$n(A)$与 $n(B)$,"排斥"$n(A\cap B)$.这由下面的事实得到.当相加$n(A)$与 $n(B)$时,我们计算 $A\cap B$ 中的元素两次.这个原理对任意个数的集合成立.我们先对 3 个集合叙述它.

定理 6.6 对任意有限集 A,B,C,有

$$n(A\cup B\cup C)=n(A)+n(B)+n(C)-n(A\cap B)-n(A\cap C)-n(B\cap C)+n(A\cap B\cap C).$$

即,"包含"$n(A)$,$n(B)$,$n(C)$,"排斥"$n(A\cap B)$,$n(A\cap C)$,$n(B\cap C)$,再包含 $n(A)\cap B\cap C$.

例 6.11 根据下列已知数据,求某院数学系学生中至少学法语、德语、俄语之一的学生数:

65 人学法语,20 人学法语和德语,

45 人学德语,25 人学法语和俄语,

42 人学俄语,15 人学德语和俄语,

8 人学所有三门语言.

要求 $n(F\cup G\cup R)$，这里 F,G,R 分别表示学法语、德语、俄语的学生的集合.

由容斥原理，

$$\begin{aligned}n(F\cup G\cup R)&=n(F)+n(G)+n(R)-n(F\cap G)-n(F\cap R)\\&\quad -n(G\cap R)+n(F\cap G\cap R)\\&=65+45+42-20-25-15+8=100.\end{aligned}$$

于是，有 100 人至少学其中一门语言.

假设 $A_1,A_2,\cdots,A_m$ 为有限集. 令 S_k 表示给定 m 个集合的所有可能的 k 个交的基数

$$n(A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k})$$

的和. 则有如下的一般的容斥原理.

定理 6.7 $n(A_1\cup A_2\cup\cdots\cup A_m)=s_1-s_2+s_3-\cdots+(-1)^{m-1}s_m$.

6.8 有序划分与无序划分

假设口袋 A 中装有编号从 1 到 7 的 7 个弹子. 计算第一次从口袋中取 2 个弹子，第 2 次从口袋中取 3 个弹子，最后从口袋中取 2 个弹子的方法数. 换句话说，求 7 个弹子集合的有序划分

$$[A_1,A_2,A_3]$$

的个数，其中 A_1 含两个弹子，A_2 含 3 个弹子，A_3 含 2 个弹子. 尽管

$$[\{1,2\},\{3,4,5\},\{6,7\}]\text{ 和 }[\{6,7\},\{3,4,5\},\{1,2\}]$$

确定了 A 的相同的划分，但我们仍将它们区别开来，因而称之为有序划分.

一开始，口袋中有 7 个弹子，因而有 $\binom{7}{2}$ 种方式取出最初的 2 个弹子，即确定 A_1；接着，口袋中余下 5 个弹子，因而有 $\binom{5}{3}$ 种方式取出 3 个弹子，即确定 A_2；最后，口袋中剩有 2 个弹子，因而有 $\binom{2}{2}$ 种方式确定 A_3. 因此 A 有

$$\binom{7}{2}\binom{5}{3}\binom{2}{2}=\frac{7\cdot 6}{1\cdot 2}\cdot\frac{5\cdot 4\cdot 3}{1\cdot 2\cdot 3}\cdot\frac{2\cdot 1}{1\cdot 2}=210$$

个不同的有序划分 $[A_1,A_2,A_3]$，其中 A_1 含 2 个弹子，A_2 含 3 个弹子，A_3 含 2 个弹子.

注意到

$$\binom{7}{2}\binom{5}{3}\binom{2}{2}=\frac{7!}{2!5!}\cdot\frac{5!}{3!2!}\cdot\frac{2!}{2!0!}=\frac{7!}{2!3!2!}.$$

因为除第 1 个分子外，每个分子被前一个因子分母中的第二项约去.

上面的讨论对一般情况也成立，即

定理 6.8 设 A 有 n 个元素，$n_1,n_2,\cdots,n_r$ 是正整数，它们的和为 n，即 $n_1+n_2+\cdots+n_r=n$. 则 A 的形如 $[A_1,A_2,\cdots,A_r]$ 的有序划分有

$$\frac{n!}{n_1!n_2!n_3!\cdots n_r!}$$

个，其中 A_1 含 n_1 个元素，A_2 含 n_2 个元素，…，A_r 含 n_r 个元素.

我们举例应用这个定理.

例 6.12 将 9 个玩具分给 4 个小朋友，若最小的小朋友分到 3 个玩具，而其他每个小朋友分到 2 个玩具. 求不同的分法数 m.

要求将 9 个玩具分成 4 份，分别含有 3,2,2,2 个玩具的有序划分数 m. 由定理 6.8

$$m=\frac{9!}{3!2!2!2!}=7560.$$

无序划分

我们常常要将集合 A 分为无序的子集类 $A_1, A_2, \cdots, A_r$. 正如 k 个对象相同时，可重排列数可由排列数除以 $k!$ 得到一样，当 k 个集合有相同的元素个数时，我们也可以用有序划分数除以 $k!$ 得到无序划分数. 我们通过下面的例子来说明，并用两种方法解决问题.

例 6.13 求 12 位学生分为 3 个队 A_1, A_2, A_3，使得每个队有 4 位学生的分法数 m.

方法一 设 A 为其中一位学生. 则有 $\binom{11}{3}$ 种方法选取另 3 位学生与 A 在同一队. 再设 B 为不与 A 在同一个队的一位学生，则有 $\binom{7}{3}$ 种方法在剩下的学生中选取 3 个学生与 B 在同一个队. 剩下的 4 位学生构成第 3 个队. 于是，划分这些学生一共有

$$m = \binom{11}{3} \cdot \binom{7}{3} = 165 \cdot 35 = 5775$$

种方法.

方法二 注意到学生的每个划分 $\{A_1, A_2, A_3\}$ 有 $3! = 6$ 种方式排成有序划分. 由定理 6.8，共有 $\frac{12!}{4!\,4!\,4!} = 34650$ 个这样的有序划分. 因此，有 $m = 34650/6 = 5775$ 个(无序)划分.

问题与解答

阶乘符号与二项式系数

6.1 计算 $4!, 5!, 6!$ 与 $7!$.

解 $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$，　$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6 \cdot (5!) = 6 \cdot (120) = 720$，

$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5 \cdot (4!) = 5 \cdot (24) = 120$，　$7! = 7 \cdot (6!) = 7 \cdot (720) = 5040$.

6.2 计算：(a) $\frac{13!}{11!}$；　(b) $\frac{7!}{10!}$.

解 (a) $\frac{13!}{11!} = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13 \cdot 12 = 156$.

还可如下求解

$$\frac{13!}{11!} = \frac{13 \cdot 12 \cdot 11!}{11!} = 13 \cdot 12 = 156.$$

(b) $\frac{7!}{10!} = \frac{7!}{10 \cdot 9 \cdot 8 \cdot 7!} = \frac{1}{10 \cdot 9 \cdot 8} = \frac{1}{720}$.

6.3 化简：(a) $\frac{n!}{(n-1)!}$；　(b) $\frac{(n+2)!}{n!}$.

解 (a) $\frac{n!}{(n-1)!} = \frac{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = n$；　或 $\frac{n!}{(n-1)!} = \frac{n(n-1)!}{(n-1)!} = n$.

(b) $\frac{(n+2)!}{n!} = \frac{(n+2)(n+1)n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = (n+2)(n+1)$

$= n^2 + 3n + 2$；

或 $\frac{(n+2)!}{n!} = \frac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2 + 3n + 2$.

6.4 计算：(a) $\binom{16}{3}$；　(b) $\binom{12}{4}$.

解 回忆分子，分母中有相同个数的因子.

(a) $\binom{16}{3} = \frac{16 \cdot 15 \cdot 14}{1 \cdot 2 \cdot 3} = 560$；　(b) $\binom{12}{4} = \frac{12 \cdot 11 \cdot 10 \cdot 9}{1 \cdot 2 \cdot 3 \cdot 4} = 495$.

6.5 计算:(a) $\binom{8}{5}$; (b) $\binom{9}{7}$.

解 (a) $\binom{8}{5}=\frac{8\cdot 7\cdot 6\cdot 5\cdot 4}{1\cdot 2\cdot 3\cdot 4\cdot 5}=56$ 或,因为 $8-5=3$,所以 $\binom{8}{5}=\binom{8}{3}=\frac{8\cdot 7\cdot 6}{1\cdot 2\cdot 3}=56$.

(b) 因为 $9-7=2$,所以 $\binom{9}{7}=\binom{9}{2}=\frac{9\cdot 8}{1\cdot 2}=36$.

6.6 证明:$\binom{17}{6}=\binom{16}{5}+\binom{16}{6}$.

证 $\binom{16}{5}+\binom{16}{6}=\frac{16!}{5!\ 11!}+\frac{16!}{6!\ 10!}$. 对两个分数通分,第一个分数乘以 $\frac{6}{6}$,第 2 个分数乘以 $\frac{11}{11}$;再相加

$$\binom{16}{5}+\binom{16}{6}=\frac{6\cdot 16!}{6\cdot 5!\cdot 11!}+\frac{11\cdot 16!}{6!\cdot 11\cdot 10!}=\frac{6\cdot 16!}{6!\cdot 11!}+\frac{11\cdot 16!}{6!\cdot 11!}$$

$$=\frac{6\cdot 16!+11\cdot 16!}{6!\cdot 11!}=\frac{(6+11)\cdot 16!}{6!\cdot 11!}=\frac{17\cdot 16!}{6!\cdot 11!}=\frac{17!}{6!\cdot 11!}=\binom{17}{6}.$$

6.7 证明定理 6.1:$\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$.

证 (证明技巧类似于上一问题.)

$\binom{n}{r-1}+\binom{n}{r}=\frac{n!}{(r-1)!\ (n-r+1)!}+\frac{n!}{r!\ \cdot(n-r)!}$,通分两个分数,第一个分数乘以 $\frac{r}{r}$,而第 2 个分数乘以 $\frac{n-r+1}{n-r+1}$,因此,

$$\binom{n}{r-1}+\binom{n}{r}=\frac{r\cdot n!}{r\cdot(r-1)!\cdot(n-r+1)!}+\frac{(n-r+1)\cdot n!}{r!\cdot(n-r+1)\cdot(n-r)!}$$

$$=\frac{r\cdot n!}{r!(n-r+1)!}+\frac{(n-r+1)\cdot n!}{r!(n-r+1)!}=\frac{r\cdot n!+(n-r+1)\cdot n!}{r!(n-r+1)!}$$

$$=\frac{[r+(n-r+1)]\cdot n!}{r!(n-r+1)!}=\frac{(n+1)n!}{r!(n-r+1)!}=\frac{(n+1)!}{r!(n-r+1)!}=\binom{n+1}{r}.$$

排列

6.8 A 与 B 之间有 4 条汽车线路. B 与 C 之间有 3 条汽车线路. 在下列 3 种情况下,一个人有多少种旅行方式?(a) 乘汽车由 A 经 B 到 C.(b) 乘汽车从 A 经 B 到 C 往返.(c) 乘汽车从 A 经 B 到 C 往返,但每个汽车线路不能超过一次.

解 (a) 有 4 种方式从 A 到 B,有 3 种方式从 B 到 C;因此,共有 $4\cdot 3=12$ 种方式从 A 经 B 到 C.

(b) 有 12 种方式从 A 经 B 到 C,且有 12 种方式返回. 因此,共有 $12\cdot 12=144$ 种方式往返旅行.

(c) 这个人从 A 到 B,到 C,到 B,再到 A 旅行. 如下记下这些字母,并用带箭头的连线连接:

$$A\rightarrow B\rightarrow C\rightarrow B\rightarrow A.$$

这个人有 4 种方式从 A 到 B,3 种方式由 B 到 C,但只能有 2 种方式从 C 到 B,有 3 种方式从 B 到 A,因为他不能用某条汽车线路超过一次. 将这些数记在上面相应箭头的上方

$$A\xrightarrow{4}B\xrightarrow{3}C\xrightarrow{2}B\xrightarrow{3}A.$$

于是,有 $4\cdot 3\cdot 2\cdot 3=72$ 种方式往返旅行,而没有汽车线路超过一次.

6.9 假设不允许重复.(a) 用 6 个数字 2,3,5,6,7,9 可以构成多少个三位数?(b) 其中有多少个数小于 400?(c) 有多少个偶数?

解 在每一情形,用 3 个方框□□□表示任意一个数. 并在每个方框中写下可放在那里的数字的个数.

(a) 左边的方框有 6 种方法填数. 接着,中间的方框有 5 种方法填数. 最后,右边的方框有 4 种方法填数:⑥⑤④. 于是,有 $6\cdot 5\cdot 4=120$ 个数.

(b) 左边的方框只有 2 种方法填数，填 2 或 3，因为每个数必须小于 400；中间的方框有 5 种方法填数；最后，右边的方框有 4 种方法填数：[2][5][4]. 于是，有 $2\cdot5\cdot4=40$ 个数.

(c) 右边的方框只有 2 种方法填数，填 2 或 6，因为必须为偶数；然后，左边的方框有 5 种填法；最后，中间的方框有 4 种填法：[5][4][2]. 于是，有 $5\cdot4\cdot2=40$ 个数.

6.10 求安排 7 人聚会的方法数：(a) 7 张椅子排成一排；(b) 围圆桌就座.

解 (a) 7 人排成一排有 $7\cdot6\cdot5\cdot4\cdot3\cdot2\cdot1=7!$ 种方法.

(b) 一人可以坐在圆桌的任一位置. 然后，其余 6 人围圆桌有 $6\cdot5\cdot4\cdot3\cdot2\cdot1=6!$ 种方法.

这是循环排列的例子. 一般地，n 个对象排成一个圆圈有 $(n-1)(n-2)\cdots3\cdot2\cdot1=(n-1)!$ 种方法.

6.11 求用下列单词的所有字母构成的不同排列的个数：(a) RADAR；(b) UNUSUAL.

解 (a) 由于有 5 个字母，其中两个 R，两个 A，所以 $\frac{5!}{2!\ 2!}=30$.

(b) 由于有 7 个字母，其中 3 个 U，所以 $\frac{7!}{3!}=840$.

6.12 有多少种方法将 4 本数学书、3 本历史书、3 本化学书和 2 本社会学书放在书架上，使得相同主题的书在一起？

解 首先，根据主题，书以 4 个单元放在书架上：□□□□. 左边的方框可以放入 4 个主题中的任一主题；第 2 个方框可以放剩下 3 个主题的任一个；第 3 个方框可以放剩下的 2 个主题之一，右边的方框放最后一个主题：[4][3][2][1]. 于是，在书架上有 $4\cdot3\cdot2\cdot1=4!$ 种方法根据主题放置书本.

在上面每个情形，数学书可以有 4! 种方法放置；历史书有 3! 种方法放置；化学书有 3! 种方法；社会学书有 2! 种方法；因此共有 $4!\cdot4!\cdot3!\cdot3!\cdot2!=41472$ 种安排.

6.13 求 n，若：(a) $P(n,2)=72$；(b) $P(n,4)=42P(n,2)$；(c) $2P(n,2)+50=P(2n,2)$.

解 (a) $P(n,2)=n(n-1)=n^2-n$；因此，$n^2-n=72$，即 $n^2-n-72=0$，即 $(n-9)(n+8)=0$. 因为 n 必须为正数，所以惟一解为 $n=9$.

(b) $P(n,4)=n(n-1)(n-2)(n-3)$，$P(n,2)=n(n-1)$. 因此，$n(n-1)(n-2)(n-3)=42n(n-1)$. 即，若 $n\neq0$，$n\neq1$，则 $(n-2)(n-3)=42$.

即 $n^2-5n+6=42$，$n^2-5n-36=0$，$(n-9)(n+4)=0$.

因为 n 必须是正的，所以仅有的答案为 $n=9$.

(c) $P(n,2)=n(n-1)=n^2-n$，$P(2n,2)=2n(2n-1)=4n^2-2n$.

因此，$2(n^2-n)+50=4n^2-2n$.

即 $2n^2-2n+50=4n^2-2n$，

即 $50=2n^2$，$n^2=25$.

由于 n 必须为正的，所以惟一解为 $n=5$.

组合

6.14 有多少种方法从 7 名男士与 5 名女士中选出由 3 名男士和 2 名女士组成的委员会？

解 从 7 名男士中选 3 名男士有 $\binom{7}{3}$ 种方法，从 5 名女士中选 2 名女士有 $\binom{5}{2}$ 种方法. 因此，有

$$\binom{7}{3}\binom{5}{2}=\frac{7\cdot6\cdot5}{1\cdot2\cdot3}\cdot\frac{5\cdot4}{1\cdot2}=350$$

种方法选出委员会.

6.15 一只口袋装有 6 个白弹子和 5 个红弹子. 求从口袋中取出 4 个弹子的方法数，使得 (a) 它们可以是任何颜色的；(b) 有 2 个白的和 2 个红的；(c) 4 个弹子同色.

解 (a) 从 11 个弹子中取（任意颜色的）4 个弹子有 $\binom{11}{4}=\frac{11\cdot10\cdot9\cdot8}{1\cdot2\cdot3\cdot4}=330$ 种方法.

(b) 取 2 个白弹子有 $\binom{6}{2}$ 种方法，取 2 个红弹子有 $\binom{5}{2}$ 种方法. 因此，有 $\binom{6}{2}\binom{5}{2}=\frac{6\cdot5}{1\cdot2}\cdot\frac{5\cdot4}{1\cdot2}=150$ 种方法取 2 个白弹子和 2 个红弹子.

(c) 取 4 个白弹子有 $\binom{6}{4}=15$ 种方法，取 4 个红弹子有 $\binom{5}{4}=5$ 种方法. 因此，共有 $15+5=20$ 种方法取出 4 个同色的弹子.

6.16 从 12 个人中可以选出多少个指定主席的 5 人委员会?

解 ☞ 主席有 12 种方法选举. 接着，委员会中的其余 4 个人从剩下的 11 人中有 $\binom{11}{4}$ 种选取方法. 于是，有 $12\cdot\binom{11}{4}=12\cdot330=3960$ 种这样的委员会.

有序划分与无序划分

6.17 有多少种方法将 9 名学生分成分别有 4 人，3 人，2 人的小组?

解 ☞ 因为每个小组的学生数不同，因而无序划分数等于有序划分数，$\frac{9!}{4!\ 3!\ 2!}=1260$.

6.18 一个班有 12 名学生. 如果 3 名学生参加一种测试，那么 12 名学生参加 4 种不同的测试有多少种方法?

解 ☞ **方法一** 求 12 名学生分成每组 3 人的有序划分数. 由定理 6.8，有 $\frac{12!}{3!\ 3!\ 3!\ 3!}=369600$ 个这样的划分.

方法二 有 $\binom{12}{3}$ 种方法选取 3 个学生参加第一种测试；接着，有 $\binom{9}{3}$ 种方法选取 3 人参加第二种测试，有 $\binom{6}{3}$ 种方法选取 3 人参加第三种测试，剩下的学生参加第四种测试. 因此，共有

$$\binom{12}{3}\binom{9}{3}\binom{6}{3}=220\cdot84\cdot20=369600$$

种方法让这些学生参加测试.

6.19 有多少种方法将 12 名学生分成 4 个组 A_1,A_2,A_3,A_4，使得每个组有 3 个学生?

解 ☞ **方法一** 注意到学生的每个划分 $\{A_1,A_2,A_3,A_4\}$ 可以安排成 $4!=24$ 个有序划分. 由于(见上一个问题)有 $\frac{12!}{3!\ 3!\ 3!\ 3!}=369600$ 个这样的有序划分，因此有 $369600/24=15400$ 个(无序)划分.

方法二 设 A 为其中一个学生. 则有 $\binom{11}{2}$ 种方法选另两位学生与 A 在同一组. 设 B 为一个与 A 不在同一组的学生. 则有 $\binom{8}{2}$ 种方法从剩下的学生中选取两位学生与 B 同一组. 再设 C 为与 A，B 不同组的一位学生. 则有 $\binom{5}{2}$ 种方法选取两位学生与 C 同组. 剩下的 3 位学生构成第 4 组，因此，共有

$$\binom{11}{2}\binom{8}{2}\binom{5}{2}=55\cdot28\cdot10=15400$$

种方法划分这些学生.

鸽笼原理

6.20 假设壁橱内有 n 双不同的鞋子. 证明：若随机地从壁橱里取出 $n+1$ 只鞋子. 则其中必有两只构成一双鞋.

证 ☞ n 双不同的鞋子构成 n 个鸽笼，$n+1$ 只鞋子相应于 $n+1$ 只鸽子，因此，一定至少有一个鸽笼中有 2 只鞋，于是，当然至少有两只是一双鞋.

6.21　假设 3 名男士和 5 名女士参加聚会，证明：若 7 人站成一排，则至少有 2 名女士相邻.

证 ☞　考虑男士不站在两端，且没有两个男士相邻的情形. 此时，3 名男士给出 4 个空档（鸽笼）供女士站立（位于两端以及男士之间的两个空档）. 由于有 5 名女士（鸽子），因此，至少有一个空档站有 2 名女士，她们必相邻. 如果男士允许相邻或在一端，则有更少的鸽笼. 因此，还是至少有 2 名女士相邻.

6.22　求至少几名学生中必有 5 人在同一个年级（一年级，二年级，三年级和四年级）.

解 ☞　$n=4$ 个年级为鸽笼，且 $k+1=5$，即 $k=4$. 因此，在任意 $kn+1=17$ 名学生（鸽子）中，必有 5 人在同一年级.

6.23　某学生必须从 3 个领域选 5 门课程. 每个学科提供大量的课程，但该学生不能在任一给定领域选超过两门课程.

(a) 用鸽笼原理证明该学生在某个领域至少选两门课程.

(b) 用容斥原理证明在每个领域，该学生必须至少选一门课程.

解 ☞　(a) 3 个领域为鸽笼，且该学生必须选 5 门课程（鸽子）. 因此，在某个领域，该学生必须至少选两门课程.

(b) 设每个领域代表三个不交的集 A,B,C. 由于集是不交的，所以 $n(A\cup B\cup C)=5=n(A)+n(B)+n(C)$. 因为在任一领域，该学生至多能选 2 门课程，因此，任两个集，比方说，A 与 B 中课程数的和一定不超过 4. 于是 $5-[n(A)+n(B)]=n(C)\geq 1$. 因而，在任一领域，该学生必须至少选一门课程.

6.24　设 L 为 26 个英文字母的表（不必按字母序），有 5 个元音 A，E，I，O，U 与 21 个辅音. (a) 证明 L 有一个子表含有 4 个或更多的相继辅音. (b) 设 L 以元音，比方说 A，开头. 证明 L 有一个子表含有 5 个或更多的相继辅音.

证 ☞　(a) 5 个字母将 L 分成 $n=6$ 个相继辅音的子表（鸽笼）. $k+1=4$，故 $k=3$. 因此，$nk+1=6\cdot 3+1=19<21$. 因此，某个子表至少有 4 个相继的辅音.

(b) 因为 L 以元音开头，剩下的元音将 L 分为 $n=5$ 个子表，$k+1=5$，故 $k=4$，因而 $kn+1=21$. 于是某个子表至少有 5 个相继的辅音.

6.25　求从 $S=\{1,2,\cdots,9\}$ 中选取的整数的最小个数 n，使得 (a) 这 n 个数中有两数之和为偶数；(b) n 个数中有两数的差是 5.

解 ☞　(a) 两偶数或两奇数之和为偶数. 将 S 的子集 $\{1,3,5,7,9\}$ 和 $\{2,4,6,8\}$ 看做鸽笼，由此 $n=3$.

(b) 将 S 的 5 个子集 $\{1,6\}$，$\{2,7\}$，$\{3,8\}$，$\{4,9\}$，$\{5\}$ 看成鸽笼. 则 $n=6$ 保证有两个整数属于同一个子集，而它们的差为 5.

容斥原理

6.26　教室里有 22 名女生和 18 名男生. 总共有多少学生？

解 ☞　男生、女生的集合是不交的；因而总数为 $t=22+18=40$ 名学生.

6.27　有 32 人回收废纸和（或）酒瓶. 其中 30 人回收废纸，14 人回收酒瓶，求人数 m，(a) 两种都回收；(b) 只回收废纸；(c) 只回收酒瓶.

解 ☞　设 P 和 B 分别表示回收废纸和酒瓶的人的集合. 由定理 6.7：

(a) $m=n(P\cap B)=n(P)+n(B)-n(P\cup B)=30+14-32=12$.

(b) $m=n(P\backslash B)=n(P)-n(P\cap B)=30-12=18$.

(c) $m=n(B\backslash P)=n(B)-n(P\cap B)=14-12=2$.

6.28　设 A,B,C,D 分别表示美术、生物、化学和戏剧课程. 根据给定数据，求集体宿舍的学生数 N：

12 人学 A，　5 人学 A 和 B，　3 人学 A，B，C，

20 人学 B，　7 人学 A 和 C，　2 人学 A，B，D，

20 人学 B，　7 人学 A 和 C，　2 人学 A,B,D，
20 人学 C，　4 人学 A 和 D，　2 人学 B,C,D，
8 人学 D，　16 人学 B 和 C，　3 人学 A,C,D，
　　　　　　4 人学 B 和 D，　2 人全学，
　　　　　　3 人学 C 和 D，　71 人全不学.

解 ☞　令 T 为至少学一门课程的学生数. 由容斥原理(定理 6.7)，$T=s_1-s_2+s_3-s_4$，

这里　$s_1=12+20+20+8=60$，　$s_2=5+7+4+16+4+3=39$，

　　$s_3=3+2+2+3=10$，　$s_4=2$.

于是 $T=29$，由此 $N=71+T=100$.

6.29　证明若 A,B 为不交的有限集，则 $A\cup B$ 是有限的，且 $n(A\cup B)=n(A)+n(B)$.

证 ☞　在计算 $A\cup B$ 的元素个数时，首先计算 A 中的元素，有 $n(A)$ 个元素. $A\cup B$ 中仅有的其余元素是那些在 B 中但不在 A 中的元素. 但由于 A 与 B 不相交. 故 B 中没有元素在 A 中，因而有 $n(B)$ 个元素在 B 中但不在 A 中，由此，

$$n(A\cup B)=n(A)+n(B).$$

6.30　对两个集合证明定理 6.7：

$$n(A\cup B)=n(A)+n(B)-n(A\cap B).$$

证 ☞　在计算 $A\cup B$ 的元素时，我们计算 A 中的元素和 B 中的元素，A 中有 $n(A)$ 个，B 中有 $n(B)$ 个. 然而，$A\cap B$ 的元素被数了两次，于是

$$n(A\cup B)=n(A)+n(B)-n(A\cap B)$$

即为所求.

　或，由不交并

$$A\cup B=A\cup(B\backslash A),\quad B=(A\cap B)\cup(B\backslash A)$$

及前一问题，有

$$n(A\cup B)=n(A)+n(B\backslash A),\quad n(B)=n(A\cap B)+n(B\backslash A).$$

于是　$n(B\backslash A)=n(B)-n(A\cap B)$.

因此，

$$n(A\cup B)=n(A)+n(B)-n(A\cap B)$$

即为所求.

补 充 题

阶乘符号

6.31　化简：(a) $\frac{(n+1)!}{n!}$；　(b) $\frac{n!}{(n-2)!}$；　(c) $\frac{(n-1)!}{(n+2)!}$；　(d) $\frac{(n-r+1)!}{(n-r-1)!}$.

6.32　求值：(a) $\binom{5}{2}$；　(b) $\binom{7}{3}$；　(c) $\binom{14}{2}$；　(d) $\binom{6}{4}$；　(e) $\binom{20}{17}$；　(f) $\binom{18}{15}$.

排列

6.33　证明：(a) $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{n}=2^n$，

(b) $\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^n\binom{n}{n}=0$.

6.34　(a) 若汽车牌照由 2 个不同的字母，紧跟着有 3 个不同的数字构成. 问有多少个汽车牌照？

(b) 若第一个数字不能为 0 呢？

6.35　在 A 和 B 之间有 6 条路，B 和 C 之间有 4 条路. 求人们能行驶的方法数：(a) 从 A 经 B 到 C；(b) 往返从 A 经 B 到 C；(c) 往返从 A 经 B 到 C，但同一条路不能超过一次.

6.36　6 个人滑一个雪橇，求其中 3 人必须驾驶雪橇的方法数.

6.37　(a) 求 5 人坐成一排的方法数.

(b) 若有两人坚持相邻而坐，则有多少种方法？

(c) 若围圆桌而坐,求解(a).

(d) 若围圆桌而坐,求解(b).

6.38 求将5本大书,4本中等书和3本小书放在书架上,使得同规格的书放在一起的方法数.

6.39 (a) 求由单词ELEVEN的字母构成的排列数.

(b) 其中有多少个以E开头和结尾.

(c) 其中有多少个排列,使得3个E连在一起?

(d) 有多少个以E开头,以N结尾?

6.40 (a) 3个男孩和2个女孩坐成一排有多少种方法?

(b) 若男孩坐在一起,女孩坐在一起呢?

(c) 若只是女孩坐在一起呢?

组 合

6.41 一名妇女有11位挚友.

(a) 她有多少种方法邀请其中五位共进午餐?

(b) 若有两人是夫妇,必须同时参加呢?

(c) 若有两人关系不好,不能同时参加呢?

6.42 一名妇女有11位好友,其中6人为女士.

(a) 她有多少种方法邀请至少3人参加聚会?

(b) 若她想要男女人数相等(包括她自己),则她有多少种方法邀请至少3人?

6.43 一次考试,一位学生要回答13个问题中的10题.

(a) 他有多少个选题方法?

(b) 若他必须回答第一、第二个问题呢?

(c) 若他必须回答第一或第二个问题(不同时回答)呢?

(d) 若他必须回答前5个问题中的正好3个问题呢?

(e) 若他必须回答前5个问题中的至少3个问题呢?

划 分

6.44 10名学生分成3个队,有多少种方法使得一个队含4名学生,另2个队含有3名学生?

6.45 将14人分为6个委员会,有多少种方法使得两个委员会含3人,其他的委员会含2人?

6.46 (a) 若允许有空子集,则有多少种方法将含有3个元素的集合划分为(i) 3个有序子集,(ii) 3个无序子集?

(b) 有多少种方法将4个元素的集合划分为(i) 3个有序子集,(ii) 3个无序子集?

杂 题

6.47 80位有车者的样本数据显示,24人有客货两用车,62人有非客货两用车.求既有客货两用车又有其他车的人数k.

6.48 设有12人读《华尔街杂志》(W)或《商业周报》(B)或两者都读.已知3人只读《华尔街杂志》,6人两者都读.求只读《商业周报》的人数k.

6.49 证明 任何7个不同的整数中,必有两个整数x和y,使得或者$x+y$或者$x-y$能被10整除.

6.50 在n个选手的竞赛中,每个选手都与其他选手比赛,每个选手至少赢一场.证明:至少有两人赢的场数相等.

补充题答案

6.31 (a) $n+1$; (b) $n(n-1)=n^2-n$; (c) $1/[n(n+1)(n+2)]$; (d) $(n-r)(n-r+1)$.

6.32 (a) 10; (b) 35; (c) 91; (d) 15; (e) 1140; (f) 816.

6.33 提示:(a) 展开$(1+1)^n$; (b) 展开$(1-1)^n$.

6.34 (a) $26\cdot25\cdot10\cdot9\cdot8=468\,000$; (b) $26\cdot25\cdot9\cdot9\cdot8=421\,200$.

6.35 (a) 24； (b) 576； (c) 360.

6.36 360.

6.37 (a) 120； (b) 48； (c) 24； (d) 12.

6.38 $3!\,5!\,4!\,3! = 103\,680$.

6.39 (a) 120； (b) 24； (c) 24； (d) 12.

6.40 (a) 120； (b) 24； (c) 48.

6.41 (a) 462； (b) 210； (c) 252.

6.42 (a) $2^{11}-1-\binom{11}{2}-\binom{11}{2}=1981$ 或 $\binom{11}{3}+\binom{11}{4}+\cdots+\binom{11}{11}=1981$.

(b) $\binom{5}{5}\binom{6}{4}+\binom{5}{4}\binom{6}{3}+\binom{5}{3}\binom{6}{2}+\binom{5}{2}\binom{6}{1}=325$.

6.43 (a) 286； (b) 165； (c) 110； (d) 80； (e) 276.

6.44 $\dfrac{10!}{4!\,3!\,3!}\cdot\dfrac{1}{2!}=2100$ 或 $\binom{10}{4}\binom{5}{2}=2100$.

6.45 $\dfrac{14!}{3!\,3!\,2!\,2!\,2!\,2!}\cdot\dfrac{1}{2!\,4!}=3\,153\,150$.

6.46 (a) (i) $3^3=27$(每个元素可放在三个部分的任一部分中).

(ii) 三个部分中元素的个数可如下分布：

(a) $[\{3\},\{0\},\{0\}]$； (b) $[\{2\},\{1\},\{0\}]$； (c) $[\{1\},\{1\},\{1\}]$.

于是,划分数为 $1+3+1=5$.

(b) (i) $3^4=81$.

(ii) 三个部分中元素的个数可如下分布：

(a) $[\{4\},\{0\},\{0\}]$； (b) $[\{3\},\{1\},\{0\}]$；

(c) $[\{2\},\{2\},\{0\}]$； (d) $[\{2\},\{1\},\{1\}]$.

于是,划分数为 $1+4+3+6=14$.

6.47 由定理 6.7,$k=62+24-80=6$.

6.48 注意到 $W\cup B=(W\setminus B)\cup(W\cap B)\cup(B\setminus W)$,且是不交并. 于是,$12=3+6+k$,即 $k=3$.

6.49 设 $X=\{x_1,x_2,x_3,\cdots,x_7\}$为 7 个不同整数的集合. r_i 为 x_i 被 10 除所得的余数. 考察 X 的划分：

$H_1=\{x_i : r_i=0\}$,　　$H_2=\{x_i : r_i=5\}$,

$H_3=\{x_i : r_i=1$ 或 $9\}$,　　$H_4=\{x_i : r_i=2$ 或 $8\}$,

$H_5=\{x_i : r_i=3$ 或 $7\}$,　　$H_6=\{x_i : r_i=4$ 或 $6\}$.

有 7 个鸽子 6 个鸽笼. 若 x 与 y 在 H_1(或 H_2)中,则 $x+y$ 与 $x-y$ 被 10 整除. 若 x 与 y 在其余 4 个子集之一,则或 $x-y$ 或 $x+y$ 被 10 整除. 但不同时被 10 整除.

6.50 每个选手赢的次数至少为 1,至多为 $n-1$. 这 $n-1$ 个数对应于 $n-1$ 个鸽笼,其不能容纳 n 个选手"鸽子". 于是,至少有两个选手赢的场数相等.

第七章 概 率 论

7.1 引 言

概率论是机会与随机性现象的一个数学模型.若随机地掷硬币,则有可能正面或反面朝上,但对某一次投掷,我们并不知道是正面还是反面朝上.用 s 表示掷 n 次硬币正面朝上的次数.随着 n 的增加,比 $f=s/n$ 变得非常稳定.这个比称为结果的*相对频数*.如果硬币非常均衡,那么可以期望正面朝上近似达到总次数的 50%,换句话说,相对频数接近$\frac{1}{2}$.也就是说,假设硬币非常均衡,则可以达到$\frac{1}{2}$.即硬币两个面出现的可能性一样;因此出现正面的机会为$\frac{1}{2}$,也就是正面朝上的概率为$\frac{1}{2}$.尽管每次掷硬币的结果是未知的,但是总体的表现是确定的.随机现象的这种长远的表现构成了概率论的基础.

随机现象的概率模型由对一个实验的每一次可能结果分配"概率"定义.对于一个给定实验,该模型的可靠性依赖于所分配的概率与极限相对频数的贴近程度.这就引出了可靠性检验问题,这属于统计学,超越了本书研究范围.

7.2 样本空间与事件

一个实验的所有可能结果的集合 S 称为*样本空间*.特定的结果,即 S 的元素称为*样本点*.*事件* A 是结果的集合.换句话说,事件 A 为样本空间的子集.特别地,由单个样本点 $a\in S$ 构成的集合$\{a\}$称为*基本事件*.此外,空集$\varnothing$与 S 本身都是事件;有时$\varnothing$称为*不可能事件*或*零事件*.

由于一个事件就是一个集合,所以利用各种集合运算可以将一些事件组合成新的事件:

(i) 事件 $A\cup B$ 发生当且仅当 A 发生或 B 发生(或同时).

(ii) 事件 $A\cap B$ 发生当且仅当 A 发生且 B 发生.

(iii) A 的补 A^c(也记为 $\overline{A}$)发生当且仅当 A 不发生.

若事件 A 与 B 是不交的,即 $A\cap B=\varnothing$,则称 A 与 B *相互排斥的*.换句话说,A 与 B 相互排斥当且仅当它们不能同时发生.如果 3 个或更多的事件两两相互排斥,那么就称这组事件相互排斥.

例 7.1 (a) 实验:掷骰子,并观察顶部出现的点数.

样本空间 S 含有 6 个可能的数,即

$$S=\{1,2,3,4,5,6\}.$$

记 A 为出现偶数事件,B 表示出现奇数事件,C 表示出现素数事件,即,设

$A=\{2,4,6\}$, $B=\{1,3,5\}$, $C=\{2,3,5\}$.

事件 $A\cup C=\{2,3,4,5,6\}$为出现偶数或素数.

事件 $B\cap C=\{3,5\}$为出现奇素数.

事件 $C^c=\{1,4,6\}$为不出现素数.

注意到 A 与 B 是相互排斥的:$A\cap B=\varnothing$.换句话说,偶数与奇数不能同时出现.

(b) 实验:掷硬币 3 次,并观察正(H)、反(T)面朝上的序列.

样本空间含有下列八个元素:

$$S=\{\text{HHH},\text{HHT},\text{HTH},\text{HTT},\text{THH},\text{THT},\text{TTH},\text{TTT}\}.$$

设 A 为至少两个相继正面朝上的事件,B 为所有投掷相同的事件,即

$$A=\{\text{HHH},\text{HHT},\text{THH}\},\quad B=\{\text{HHH},\text{TTT}\}.$$

那么 $A\cap B=\{\text{HHH}\}$为仅出现正面朝上的事件.五个正面朝上的事件为空集$\varnothing$.

(c) 实验:掷硬币直至正面朝上.统计掷硬币的次数.

该实验的样本空间 $S=\{1,2,3,\cdots\}$. 由于每个正整数都是 S 的元素,故样本空间是无限的.

注 7.1(c)的样本空间不是有限的.有关这种样本空间的理论超出本书的范围.由此,除非注明,所有样本空间都是有限的.

7.3 有限概率空间

采用下面的定义.

定义 设 S 为有限样本空间,$S=\{a_1,a_2,\cdots,a_n\}$,若对 S 的每个点 a_i 指定一个实数 p_i,称为 a_i 的概率,且满足下列性质:

(i) 每个 p_i 非负,即 $p_i \geqslant 0$.

(ii) 所有 p_i 的和为1,即 $p_1+p_2+\cdots+p_n=1$.

则称为有限概率空间,或称为概率模型.事件 A 的概率记为 $P(A)$,定义为 A 中点的概率之和.

单元素集 $\{a_i\}$ 称为基本事件,为方便,用 $P(a_i)$ 代替 $P(\{a_i\})$.

例 7.2 实验:掷3枚硬币,并观察正面朝上的个数.[比较上面的例子7.1(b).]

样本空间 $S=\{0,1,2,3\}$. 对 S 的元素的下述指派定义了一个概率空间:

$$P(0)=\frac{1}{8},\quad P(1)=\frac{3}{8},\quad P(2)=\frac{3}{8},\quad P(3)=\frac{1}{8}.$$

即,每个概率是非负的,且概率的和为1.设 A 为至少一个正面朝上的事件,B 为所有正面朝上或所有反面朝上的事件,即 $A=\{1,2,3\}$,$B=\{0,3\}$.则由定义知

$$P(A)=P(1)+P(2)+P(3)=\frac{3}{8}+\frac{3}{8}+\frac{1}{8}=\frac{7}{8},$$

$$P(B)=P(0)+P(3)=\frac{1}{8}+\frac{1}{8}=\frac{1}{4}.$$

等概率空间

实验的自然特征常常要求样本空间的各种结果具有相等的概率.这样的有限概率空间,即每个样本点有相同的概率的有限概率空间称为等概率空间.特别地,若 S 有 n 个点,则每个点的概率为 $\frac{1}{n}$.进一步,若事件 A 有 r 个点,则它的概率为 $r\cdot\frac{1}{n}=\frac{r}{n}$.换句话说

$$P(A)=\frac{A\text{ 中元素个数}}{S\text{ 中元素个数}}=\frac{n(A)}{n(S)},\quad \text{或}\quad P(A)=\frac{\text{有利于 }A\text{ 的结果数}}{\text{全部可能结果数}},$$

这里 $n(A)$ 表示 A 中元素的个数.

注意上面 $P(A)$ 的公式仅适用于等概率空间,一般不能成立.

术语随机仅用于等概率空间:"从 S 中随机地选取一点"是指 S 中的每个样本点有相同的被选取概率.

例 7.3 从一副52张普通纸牌中抽取一张纸牌,设

$$A=\{\text{这张牌为黑桃}\},\quad B=\{\text{这张牌为大牌}\},$$

(大牌是指 J,Q,K.)我们来计算 $P(A)$,$P(B)$ 和 $P(A\cap B)$.因为是等概率空间,故

$$P(A)=\frac{\text{黑桃的张数}}{\text{牌的张数}}=\frac{13}{52}=\frac{1}{4},\quad P(B)=\frac{\text{大牌的张数}}{\text{牌的张数}}=\frac{12}{52}=\frac{3}{13},$$

$$P(A\cap B)=\frac{\text{黑桃大牌的张数}}{\text{牌的张数}}=\frac{3}{52}.$$

有关有限概率空间的定理

直接利用每个事件的概率就是其点的概率之和这个事实,可得下面的定理.

定理 7.1　定义在有限概率空间 S 所有事件点上的概率函数 P 有如下性质：

[**P1**]　对每个事件 A，$0\leqslant P(A)\leqslant 1$.

[**P2**]　$P(S)=1$.

[**P3**]　若事件 A,B 相互排斥，则

$$P(A\cup B)=P(A)+P(B).$$

下面的定理使我们的直觉正式化：若 P 是事件 E 发生的概率，则 $1-P$ 是事件 E 不发生的概率.（即，若我们有次数的 $P=\frac{1}{3}$ 击中目标，则就有次数的 $1-P=\frac{2}{3}$ 偏离目标）

定理 7.2　设 A 为任一事件，则 $P(A^c)=1-P(A)$.

由定理 7.1 可直接推得下面的定理（由问题 7.16 证明）.

定理 7.3　设 $\varnothing$ 为空集. A,B 为任意两个事件，则

(i) $P(\varnothing)=0$.

(ii) $P(A\backslash B)=P(A)-P(A\cap B)$.

(iii) 若 $A\subseteq B$，则 $P(A)\leqslant P(B)$.

注意到定理 7.1 中的性质[**P3**]给出了在所有事件不相交的情形下事件并的概率. 一般的公式（在问题 7.17 中证明）称为加法原理.

定理 7.4（加法原理）　对任何事件 A 与 B，有

$$P(A\cup B)=P(A)+P(B)-P(A\cap B).$$

例 7.4　100 名学生中有 30 名学数学，20 名学化学，10 名学数学和化学. 从中随机地选出一名学生，求该学生学数学或化学的概率 p.

设 $M=\{$学数学的学生$\}$，$C=\{$学化学的学生$\}$. 由于空间是等概率的，所以

$$P(M)=\frac{30}{100}=\frac{3}{10},P(C)=\frac{20}{100}=\frac{1}{5},$$

$$P(M\text{与}C)=P(M\cap C)=\frac{10}{100}=\frac{1}{10}.$$

于是，由加法原理（定理 7.4）得，

$$p=P(M\text{或}C)=P(M\cup C)=P(M)+P(C)-P(M\cap C)$$
$$=\frac{3}{10}+\frac{1}{5}-\frac{1}{10}=\frac{2}{5}.$$

7.4　条件概率

设 E 为概率空间 S 的一个事件，$P(E)>0$. 在 E 已发生的条件下，事件 A 发生的概率，即在 E 发生的条件下，A 的条件概率，记为 $P(A|E)$. 定义如下

$$P(A\mid E)=\frac{P(A\cap E)}{P(E)}.$$

正如 Venn 图 7-1，在某些意义下，$P(A|E)$ 给出了 A 关于诱导空间 E 的相对概率.

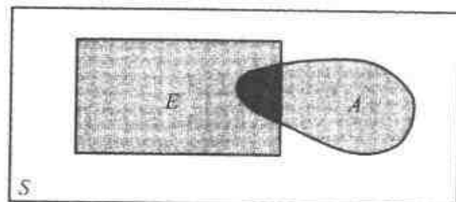


图 7-1

设 S 为等概率空间，$n(A)$ 表示事件 A 的元素个数，则

$$P(A\cap E)=\frac{n(A\cap E)}{n(S)},\quad P(E)=\frac{n(E)}{n(S)}.$$

因此，

$$P(A \mid E)=\frac{P(A \cap E)}{P(E)}=\frac{n(A \cap E)}{n(E)}.$$

下面将这个结果正式地叙述出来.

定理 7.5 设 S 为等概率空间，A,E 为两个事件，则

$$P(A \mid E)=\frac{A \cap E\text{ 中元素个数}}{E\text{ 中元素个数}}=\frac{n(A \cap E)}{n(E)}.$$

例 7.5 (a) 掷一对相当的骰子. 样本空间 S 由 36 个有序偶(a,b)构成，其中 a 和 b 可以为 1 到 6 的任何整数(见问题 7.3). 于是，任意点的概率为$\frac{1}{36}$. 求和为 6 时，一个骰子是 2 的概率. 即求 $P(A|E)$. 这里，

$$E=\{\text{和为 }6\}, A=\{\text{至少有一个为 }2\}.$$

也求 $P(A)$.

E 由 5 个元素组成，特别地，

$$E=\{(1,5),(2,4),(3,3),(4,2),(5,1)\}.$$

其中两个(2,4)和(4,2)属于 A，即

$$A \cap E=\{(2,4),(4,2)\}.$$

由定理 7.5，$P(A|E)=\frac{2}{5}$.

另一方面，A 有 11 个元素，特别地

$$A=\{(2,1),(2,2),(2,3),(2,4),(2,5),(2,6),\\(1,2),(3,2),(4,2),(5,2),(6,2)\}.$$

而 S 有 36 个元素，因此，$P(A)=\frac{11}{36}$.

(b) 一对夫妇有两个孩子. 样本空间 $S=\{bb,bg,gb,gg\}$，每个样本点概率为$\frac{1}{4}$. 如果已知

(i) 至少一个是男孩，

(ii) 大的孩子为男孩.

求两个孩子都是男孩的概率 p.

(i) 诱导空间由 3 个元素组成：$\{bb,bg,gb\}$. 因此，$p=\frac{1}{3}$.

(ii) 诱导空间只有 2 个元素：$\{bb,bg\}$，因此，$p=\frac{1}{2}$.

条件概率的乘法定理

设 A,B 为样本空间 S 的两个事件，$P(A)>0$. 由条件概率的定义

$$P(B \mid A)=\frac{P(A \cap B)}{P(A)}$$

两边同乘以 $P(A)$就得到下面有用的结论.

定理 7.6(条件概率的乘法定理) $P(A \cap B)=P(A)P(B|A)$.

乘法定理给出了求两事件 A 与 B 都发生的概率的公式. 容易推广到 3 个或多个事件 A_1，$A_2,\cdots,A_m$；即

$$P(A_1 \cap A_2 \cap \cdots \cap A_m)=P(A_1)\cdot P(A_2 \mid A_1)\cdots P(A_m \mid A_1 \cap A_2 \cap \cdots \cap A_{m-1}).$$

例 7.6 一批产品有 12 件，其中 4 件为次品. 随机地从这批产品中依次抽取 3 件. 求 3 个都不是次品的概率 p.

第一件不是次品的概率为$\frac{8}{12}$，因为 12 件产品中有 8 件不是次品. 若第一件不是

次品，则第二件不是次品的概率为$\frac{7}{11}$，因为剩下的11件产品中只有7件不是次品. 若第一、二件不是次品，则最后一件不是次品的概率为$\frac{6}{10}$，因为剩下的10件产品中只有6件不是次品. 于是，由乘法定理得

$$p=\frac{8}{12}\cdot\frac{7}{11}\cdot\frac{6}{10}=\frac{14}{55}\approx 0.25.$$

7.5 独立事件

设A,B为概率空间S的两个事件，若一个事件的发生并不影响另一个事件的发生，则称它们是独立的. 更确切地，若$P(B)$与$P(B|A)$相同，则B与A独立. 在乘法定理$P(A\cap B)=P(A)P(B|A)$中用$P(B)$代替$P(B|A)$可得

$$P(A\cap B)=P(A)P(B).$$

我们用上面的等式作为独立性的正式定义.

定义 若$P(A\cap B)=P(A)P(B)$，则称事件A与B为独立的，否则称为相关的.

应该指出，独立性是一个对称关系，特别地，等式$P(A\cap B)=P(A)P(B)$蕴含了

$$P(B\mid A)=P(B)\quad 与\quad P(A\mid B)=P(A).$$

例7.7 掷硬币三次给出等概率空间

$$S=\{\text{HHH},\text{HHT},\text{HTH},\text{HTT},\text{THH},\text{THT},\text{TTH},\text{TTT}\}.$$

考虑事件：

$$A=\{第一次正面朝上\}=\{\text{HHH},\text{HHT},\text{HTH},\text{HTT}\}$$

$$B=\{第二次正面朝上\}=\{\text{HHH},\text{HHT},\text{THH},\text{THT}\}$$

$$C=\{恰相连两次正面朝上\}=\{\text{HHT},\text{THH}\}.$$

显然，A与B是独立事件；下面将给出证明. 另一方面，A与C，B与C之间的关系并不明显. 我们证明A与C是独立的，但B与C是相关的. 首先

$$P(A)=\frac{4}{8}=\frac{1}{2},P(B)=\frac{4}{8}=\frac{1}{2},P(C)=\frac{2}{8}=\frac{1}{4}.$$

再者，

$$P(A\cap B)=P(\{\text{HHH},\text{HHT}\})=\frac{1}{4},$$

$$P(A\cap C)=P(\{\text{HHT}\})=\frac{1}{8},$$

$$P(B\cap C)=P(\{\text{HHT},\text{THH}\})=\frac{1}{4}.$$

因此，

$$P(A)P(B)=\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}=P(A\cap B)，由此，A与B独立.$$

$$P(A)P(C)=\frac{1}{2}\cdot\frac{1}{4}=\frac{1}{8}=P(A\cap C)，由此，A与C独立.$$

$$P(B)P(C)=\frac{1}{2}\cdot\frac{1}{4}=\frac{1}{8}\neq P(B\cap C)，由此，B与C相关.$$

我们常常假定两事件是独立的，或者实验本身蕴含了两个事件是独立的.

例7.8 A击中目标的概率为$\frac{1}{4}$，B击中目标的概率为$\frac{2}{5}$. 两人射击目标，求至少一人击中目标的概率，即A或B(或两人都)击中目标的概率.

已知$P(A)=\frac{1}{4}$，$P(B)=\frac{2}{5}$. 求$P(A\cup B)$. 再者，A或B击中目标的概率不受另

一人击中目标的影响;即 A 击中目标与 B 击中目标独立,即 $P(A\cap B)=P(A)P(B)$,因此,

$$P(A\cup B)=P(A)+P(B)-P(A\cap B)=P(A)+P(B)-P(A)P(B)$$
$$=\frac{1}{4}+\frac{2}{5}-\left(\frac{1}{4}\right)\left(\frac{2}{5}\right)=\frac{11}{20}.$$

7.6 独立重复试验,二项分布

前面已讨论与有限次重复试验有关的概率空间,如掷硬币三次.下面给出重复的概念.

定义 设 S 为有限概率空间.称 S 的有序 n 元组构成的概率空间 S_n 为 n 个独立重复试验的空间,且 n 元组的概率定义为其每个分量的概率的乘积:

$$P((s_1,s_2,\cdots,s_n))=P(s_1)P(s_2)\cdots P(s_n).$$

例 7.9 3 匹马 a,b,c 一起赛跑,它们各自获胜的概率为 $\frac{1}{2},\frac{1}{3}$ 和 $\frac{1}{6}$.换言之,$S=\{a,b,c\}$,

$P(a)=\frac{1}{2},P(b)=\frac{1}{3},P(c)=\frac{1}{6}$.如果比赛两次,则两次重复试验的样本空间为

$$S_2=\{aa,ab,ac,ba,bb,bc,ca,cb,cc\}.$$

为方便书写,将有序偶(a,c)写为 ac. S_2 中每个点的概率为

$$P(aa)=P(a)P(a)=\frac{1}{2}\left(\frac{1}{2}\right)=\frac{1}{4},\quad P(ba)=\frac{1}{6},\quad P(ca)=\frac{1}{12},$$
$$P(ab)=P(a)P(b)=\frac{1}{2}\left(\frac{1}{3}\right)=\frac{1}{6},\quad P(bb)=\frac{1}{9},\quad P(cb)=\frac{1}{18},$$
$$P(ac)=P(a)P(c)=\frac{1}{2}\left(\frac{1}{6}\right)=\frac{1}{12},\quad P(bc)=\frac{1}{18},\quad P(cc)=\frac{1}{36}.$$

因此,c 胜第一场,a 胜第二场的概率为 $P(ca)=\frac{1}{12}$.

两个结果的重复试验,Bernoulli 试验

考察只有两个结果的试验.这样的独立重复试验称为 Bernoulli 试验,是以瑞士数学家 I. Bernoulli (1654~1705)的名字命名的.独立试验是指任何试验的结果不依赖于前一结果(如,掷硬币).我们称一个结果为*成功*,另一结果为*失败*.

设 p 表示 Bernoulli 试验中成功的概率,因此,失败的概率为 $q=1-p$. *二项试验*由一组 Bernoulli 试验构成,符号 $B(n,p)$表示 n 个试验,且成功概率为 p 的二项试验.

我们常常对二项试验中成功的次数感兴趣,而并不关心他们出现的次序.有下面的定理(在问题 7.38 中证明).

定理 7.7 在二项试验 $B(n,p)$中恰有 k 次成功的概率为

$$p(k)=P(k\text{ 个成功})=\binom{n}{k}p^kq^{n-k}.$$

一次或更多次成功的概率为 $1-q^n$.

这里$\binom{n}{k}$为二项式系数,已在第六章中定义和讨论.

例 7.10 掷硬币 6 次,称正面朝上为成功.这是 $n=6,p=q=\frac{1}{2}$的二项试验.

(a) 恰出现两次正面的概率(即 $k=2$)为

$$P(2)=\binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4=\frac{15}{64}\approx 0.23.$$

(b) 至少 4 次正面的概率(即 $k=4,5,6$)为

$$P(4)+P(5)+P(6)=\binom{6}{4}\left(\frac{1}{2}\right)^4\left(\frac{1}{2}\right)^2+\binom{6}{5}\left(\frac{1}{2}\right)^5\left(\frac{1}{2}\right)+\binom{6}{6}\left(\frac{1}{2}\right)^6$$

$$=\frac{15}{64}+\frac{6}{64}+\frac{1}{64}=\frac{11}{32}\approx 0.34.$$

(c) 未出现正面(即全失败)的概率为 $q^6=\left(\frac{1}{2}\right)^6=\frac{1}{64}$,因此,一次或更多次正面朝上的概率为 $1-q^n=1-\frac{1}{64}=\frac{63}{64}\approx 0.94$.

注 二项试验 $B(n,p)$ 的函数 $P(k)$、$k=0,1,2,\cdots,n$ 称为二项分布. 因为它对应于二项展开式的相继项:

$$(q+p)^n=q^n+\binom{n}{1}q^{n-1}p+\binom{n}{2}q^{n-2}p^2+\cdots+p^n.$$

在本章的后面再解释术语分布的用处.

7.7 随机变量

设 S 为一个实验的样本空间. 如前所述,实验的结果或 S 的点不必为数. 例如,掷硬币时,结果为正面 H 或反面 T;掷一对骰子时,结果为整数对. 然而,我们常希望对实验的每个结果指定一个数. 例如,掷硬币时,可指定 H 为 1,T 为 0;掷一对骰子时,对结果指定两整数的和. 这样的数值指派称为随机变量. 更一般地,有如下定义:

定义 随机变量 X 为一个法则,它对样本空间 S 的每个结果指定一个数值.

用 R_X 表示由随机变量 X 指定的数的集合. 也称 R_X 为范围空间.

注 更正式地说,X 为从 S 到实数 $\mathbf{R}$ 的一个函数,R_X 为 X 的值域. 对某些无限样本空间 S,也并不是所有从 S 到 $\mathbf{R}$ 的函数都可认为随机变量. 然而,这里的样本空间是有限的,且定义在有限样本空间上的每个实值函数都是随机变量.

例 7.11 掷一对骰子.(见问题 7.3). 样本空间由 36 个有序偶 (a,b) 构成,这里 a,b 可以是 1 到 6 的任意整数,即,

$$S=\{(1,1),(1,2),\cdots,(6,6)\}.$$

设 X 指定 S 的每个点为两数之和. 则 X 为随机变量,具有范围空间

$$R_X=\{2,3,4,5,6,7,8,9,10,11,12\}.$$

设 Y 指定每个点为两数中的最大数. 则 Y 为随机变量,具有范围空间

$$R_Y=\{1,2,3,4,5,6\}.$$

例 7.12 一个盒子装有 12 件产品,其中 3 件是次品. 从盒中取 3 件为一个样品. 样品空间 S 由 $\binom{12}{3}=220$ 个不同的 3 个元素的样本构成. 设 X 为该样本中次品的数量. 则 X 为随机变量,具有范围空间 $R_X=\{0,1,2,3\}$.

随机变量的概率分布

设 $R_X=\{x_1,x_2,\cdots,x_t\}$ 为定义在有限样本空间 S 上的随机变量 X 的范围空间. 则 X 诱导出范围空间 R_X 的概率指派:

$p_i=P(x_i)=P(X=x_i)=S$ 中像为 x_i 的点的概率之和.

有序偶 $(x_1,p_1),\cdots,(x_t,p_t)$ 的集合,常用一张表表示:

x_1	x_2	$\cdots$	x_t
p_1	p_2	$\cdots$	p_t

称为随机变量 X 的分布.

当 S 为等概率空间时，容易从下面的结果得到随机变量分布.

定理 7.8　设 S 为等概率空间，X 为 S 上的随机变量，具有范围空间 $R_X=\{x_1,x_2,\cdots,x_t\}$. 则

$$p_i = P(x_i) = \frac{S\text{ 中像为 } x_i \text{ 的点数}}{S\text{ 中的点数}}$$

例 7.13　考察例 7.11 的随机变量 X，它将和指定给掷一对骰子. 利用定理 7.8 求 X 的分布.

和为 2 的结果仅一个(1,1)；因此 $P(2)=\frac{1}{36}$. 和为 3 的结果有两个，(1,2)和(2,1)；因此 $P(3)=\frac{2}{36}$. 和为 4 的结果有 3 个，(1,3)，(2,2)，(3,1)；因此，$P(4)=\frac{3}{36}$. 类似地，$P(5)=\frac{4}{36}$，$P(6)=\frac{5}{36}$，…，$P(12)=\frac{1}{36}$. X 的分布由 R_X 中的点及其概率构成，即

x_i	2	3	4	5	6	7	8	9	10	11	12
p_i	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

例 7.14　设 X 为例 7.12 的随机变量. 利用定理 7.8 求 X 的分布.

无次品的 3-元样本有 $\binom{9}{3}=84$ 个，因此 $P(0)=\frac{84}{220}$. 含一个次品的 3-元样本有 $3\cdot\binom{9}{2}=108$ 个，因此，$P(1)=\frac{108}{220}$. 含两个次品的 3-元样本有 $\binom{3}{2}\cdot 9=27$ 个，因此，$P(2)=\frac{27}{220}$. 含 3 个次品的 3-元样本只有一个，因此 $P(3)=\frac{1}{220}$. 由此得 X 的分布：

x_i	0	1	2	3
p_i	$\frac{84}{220}$	$\frac{108}{220}$	$\frac{27}{220}$	$\frac{1}{220}$

注　设 X 为概率空间 $S=\{a_1,a_2,\cdots,a_m\}$ 的随机变量，$f(X)$ 是多项式. 则 $f(X)$ 为随机变量，其指派 $f(X(a_i))$ 到点 a_i. 即 $f(X)(a_i)=f(X(a_i))$. 因此，若 X 取值 $x_1,x_2,\cdots,x_n$ 的各自概率为 $p_1,p_2,\cdots,p_n$，则 $f(x)$ 取值 $f(x_1),f(x_2),\cdots,f(x_n)$ 具有相同的对应概率.

随机变量的期望

设 X 为随机变量. 关于 X 有两个重要的度量(参数)：X 的均值，记为 μ 或 μ_X；和 X 的标准差记为 σ 或 σ_X. 均值 μ 也称为 X 的期望，记为 $E(X)$. 在一定意义上，均值 μ 测量了 X 的"中心趋向". 而标准差测量了 X 的"扩展"或"弥散". (均值有时也称为平均值，因为它对应着一组数的平均值. 而一个数的概率为该数在这组数中的相对频数.) 本小节讨论 X 的期望 $\mu=E(X)$，下节讨论 X 的标准差 σ.

设 X 为概率空间 $S=\{a_1,a_2,\cdots,a_m\}$ 上的随机变量，X 的均值或期望如下定义

$$\mu = E(X) = X(a_1)P(a_1)+X(a_2)P(a_2)+\cdots+X(a_m)P(a_m) = \sum X(a_i)P(a_i).$$

特别地，若已知 X 的分布

x_1	x_2	…	x_n
p_1	p_2	…	p_n

则 X 的期望为

$$\mu = E(X) = x_1p_1+x_2p_2+\cdots+x_np_n = \sum x_ip_i.$$

(为方便,省略求和符号中的上下限).

例 7.15 (a) 掷硬币 6 次.正面朝上的次数及其概率如下:

x_i	0	1	2	3	4	5	6
p_i	$\frac{1}{64}$	$\frac{6}{64}$	$\frac{15}{64}$	$\frac{20}{64}$	$\frac{15}{64}$	$\frac{6}{64}$	$\frac{1}{64}$

那么正面朝上的均值或期望或期望值为

$$\mu = E(X) = 0\left(\frac{1}{64}\right)+1\left(\frac{6}{64}\right)+2\left(\frac{15}{64}\right)+3\left(\frac{20}{64}\right)+4\left(\frac{15}{64}\right)+5\left(\frac{6}{64}\right)+6\left(\frac{1}{64}\right)$$
$$= 3.$$

(b) 考察例 7.12 中的随机变量 X,其分布在例 7.14 中.它给出了在 3-元样本中次品的可能件数及其概率.那么 X 的期望,即 3-元样品中次品的期望值为

$$\mu = E(X) = 0\left(\frac{84}{220}\right)+1\left(\frac{108}{220}\right)+2\left(\frac{27}{220}\right)+3\left(\frac{1}{220}\right) = 0.75.$$

(c) 3 匹马 a,b,c 参加比赛,设它们各自的获胜概率为 $\frac{1}{2}$,$\frac{1}{3}$ 和 $\frac{1}{6}$.再设 X 为获胜马匹的支付函数,且 a,b,c 获胜分别支付 2 美元、6 美元、9 美元.则比赛的期望支付为

$$E(X) = X(a)P(a)+X(b)P(b)+X(c)P(c)$$
$$= 2\left(\frac{1}{2}\right)+6\left(\frac{1}{3}\right)+9\left(\frac{1}{6}\right) = 4.5.$$

随机变量的方差与标准差

考察随机变量 X,其均值为 μ,概率分布为

x_1	x_2	x_3	$\cdots$	x_n
p_1	p_2	p_3	$\cdots$	p_n

如下定义 X 的*方差* $\mathrm{Var}(X)$与标准差 σ:

$$\mathrm{Var}(X) = (x_1-\mu)^2p_1+(x_2-\mu)^2p_2+\cdots+(x_n-\mu)^2p_n = \sum(x_i-\mu)^2p_i$$
$$= E((X-\mu)^2),$$
$$\sigma = \sqrt{\mathrm{Var}(X)}.$$

下面的公式在计算 $\mathrm{Var}(X)$时常常比上面的定义更方便:

$$\mathrm{Var}(X) = x_1^2p_1+x_2^2p_2+\cdots+x_n^2p_n-\mu^2 = \sum x_i^2p_i-\mu^2 = E(X^2)-\mu^2.$$

注 由上面的公式,$\mathrm{Var}(X)=\sigma^2$,σ^2 与 σ 都测量了诸 x_i 对均值 μ 的偏离程度;然而,σ 与 μ 有相同的单位.

例 7.16 (a) 掷硬币 6 次,X 表示正面朝上的次数.例 7.15(a)给出了 X 的分布,并计算了均值 $\mu=3$. X 的方差可如下计算:

$$\mathrm{Var}(X) = (0-3)^2\frac{1}{64}+(1-3)^2\frac{6}{64}+(2-3)^2\frac{15}{64}$$
$$+\cdots+(6-3)\frac{1}{64} = 1.5.$$

或,

$$\mathrm{Var}(X) = 0^2\frac{1}{64}+1^2\frac{6}{64}+2^2\frac{15}{64}+3^2\frac{20}{64}+4^2\frac{15}{64}$$
$$+5^2\frac{6}{64}+6^2\frac{1}{64}-3^2 = 1.5$$

因此,标准差为 $\sigma=\sqrt{1.5}\approx 1.225$(正面朝上).

(b) 考察例 7.15(b)中的随机变量 X,已计算均值 $\mu=0.75$.(其分布出现在例 7.14 中)X 的方差计算如下:

$$\mathrm{Var}(X)=0^2\frac{84}{220}+1^2\frac{108}{220}+2^2\frac{27}{220}+3^2\frac{1}{220}-(0.75)^2=0.46.$$

于是,标准差为

$$\sigma=\sqrt{\mathrm{Var}(X)}=\sqrt{0.46}\approx 0.68.$$

二项分布

考虑二项试验 $B(n,p)$,即 $B(n,p)$由 n 个独立重复试验构成,每个试验有两个结果:成功与失败,p 为成功的概率.k 次成功数 X 是一个随机变量,其分布如图 7-2.

k	0	1	2	…	n
$P(k)$	q^n	$\binom{n}{1}q^{n-1}p$	$\binom{n}{2}q^{n-2}p^2$	…	p^n

图 7-2

下面的定理是实用的

定理 7.9 考察二项分布 $B(n,p)$.则

(i) 期望值 $E(X)=\mu=np$.

(ii) 方差 $\mathrm{Var}(X)=\sigma^2=npq$.

(iii) 标准差 $\sigma=\sqrt{npq}$.

例 7.17 (a) 某男子击中目标的概率为 $p=\frac{1}{5}$.他射击 100 次,求他击中目标数的期望值 μ 及标准差 σ.

这里 $p=\frac{1}{5}$,由此 $q=\frac{4}{5}$.因此

$$\mu=np=100\cdot\frac{1}{5}=20,\quad \sigma=\sqrt{npq}=\sqrt{100\cdot\frac{1}{5}\cdot\frac{4}{5}}=4.$$

(b) 求通过猜测 5 个判断题答案而得到的正确答案数的期望值 $E(X)$.

这里 $p=\frac{1}{2}$.因此 $E(X)=np=5\cdot\frac{1}{2}=2.5$.

问题与解答

样本空间与事件

7.1 设 A,B 为两个事件.求下列事件的表示式,并画出 Venn 图:

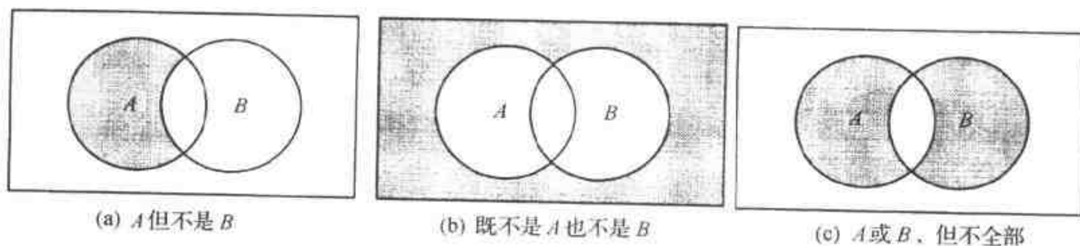
(a) A 但不是 B; (b) 既不是 A 也不是 B;

(c) 或者 A,或者 B,但不全部.

解 (a) 因 A 发生但 B 不发生.给 A 内但在 B 外的区域涂阴影.如图 7-3(a).由于 B 不发生,所以 B 的补 B^c 发生.因此 A 与 B^c 发生.换句话说该事件为 $A\cap B^c$.

(b) "既不是 A 也不是 B"是指"非 A 非 B",即 $A^c\cap B^c$,由 De Morgan 律,也即 $(A\cup B)^c$.因此,给 A 和 B 的外部,即 $A\cup B$ 的外部涂阴影,如图 7-3(b).

(c) 由于 A 或 B 发生,但 A,B 不同时发生,给 A 与 B 的区域,公共部分除外涂上阴影.如图 7-3(c).该事件等价于 A 发生但 B 不发生,或 B 发生但 A 不发生.因此,该事件为 $(A\cap B^c)\cup(B\cap A^c)$.



(a) A但不是B (b) 既不是A也不是B (c) A或B，但不全部

图 7-3

7.2 掷一枚硬币和一个骰子，样本空间 S 由 12 个元素构成：

$$S=\{H1,H2,H3,H4,H5,H6,T1,T2,T3,T4,T5,T6\}.$$

(a) 准确表达下列事件：

$A=$ {正面与一个偶数出现}.

$B=$ {出现一个素数}.

$C=$ {反面与一个奇数出现}.

(b) 准确表达事件：(i) A 或 B 发生；(ii) B 与 C 发生；(iii) 仅 B 发生.

(c) A,B,C 中哪一对事件相互排斥？

解 (a) A 的元素就是 S 中由一个 H 和一个偶数构成的元素：

$$A=\{H2,H4,H6\}.$$

B 的元素就是 S 中第二个分量为素数的那些点：

$$B=\{H2,H3,H5,T2,T3,T5\}.$$

C 的元素为 S 中由一个 T 和一个奇数构成的那些点：

$$C=\{T1,T3,T5\}.$$

(b) (i) $A\cup B=\{H2,H4,H6,H3,H5,T2,T3,T5\}$.

(ii) $B\cap C=\{T3,T5\}$.

(iii) $B\cap A^c\cap C^c=\{H3,H5,T2\}$.

(c) 因为 $A\cap C=\varnothing$，所以 A 与 C 相互排斥.

7.3 掷一对骰子，并记录上面的两个数，描述样本空间 S，并求 S 中元素的个数 $n(S)$.

解 每个骰子上有 6 个可能的数：1,2,…,6. 因此 $n(S)=6\cdot 6=36$，且 S 由 1～6 的 36 个数对构成. 图 7-4 给出了这 36 个数对，且每行有相同的第一个元素，每列有相同的第 2 个元素.

(1,1),(1,2),(1,3),(1,4),(1,5),(1,6)
(2,1),(2,2),(2,3),(2,4),(2,5),(2,6)
(3,1),(3,2),(3,3),(3,4),(3,5),(3,6)
(4,1),(4,2),(4,3),(4,4),(4,5),(4,6)
(5,1),(5,2),(5,3),(5,4),(5,5),(5,6)
(6,1),(6,2),(6,3),(6,4),(6,5),(6,6)

图 7-4

7.4 考察问题 7.3 中的样本空间 S. 求下列每个事件中元素的个数：

(a) $A=$ {两数相等}.

(b) $B=$ {两数的和至少为 10}.

(c) $C=$ {第一个骰子上出现 5}.

(d) $D=$ {至少一个骰子出现 5}.

(e) $E=$ {两数之和至多为 7}.

解 利用图 7-4 有助于计算事件中元素的个数：

(a) $A=\{(1,1),(2,2),\cdots,(6,6)\}$，因此 $n(A)=6$.

(b) $B=\{(6,4),(5,5),(4,6),(6,5),(5,6),(6,6)\}$，因此，$n(B)=6$.

(c) $C=\{(5,1),(5,2),\cdots,(5,6)\}$，因此，$n(C)=6$.

(d) 5 作为第一个元素有 6 个数偶，作为第 2 个元素也有 6 个数偶. 而(5,5)两种情况都算一次. 因此 $n(D)=6+6-1=11$.

或，计数图 7-4 中属于 D 的元素得到 $n(D)=11$.

(e) 设 $n(s)$ 表示 S 中和为 s 的数偶的个数，和为 7 出现在图 7-4 数阵的对角线上；因此 $n(7)=6$. 和为 6 正好出现在对角线的上面，因此 $n(6)=5$. 类似地，$n(5)=4$，$n(3)=2$，$n(2)=1$，因此，

$$n(E)=6+5+4+3+2+1=21$$

或，$n(7)=6$ 且剩下 $36-6=30$ 个数偶，其中一半和大于 7，一半和小于 7. 因此，$n(E)=6+15=21$.

有限等概率空间

7.5 求每个事件的概率 p：

(a) 掷一个骰子出现偶数.

(b) 掷 3 个硬币至少一次正面朝上.

(c) 一个盒子装有 4 个白弹子，3 个红弹子和 5 个蓝弹子，从该盒中随机抓出一个弹子为红弹子.

解 ☞ 每个样本空间 S 为等概率空间. 因此，对每个事件 E，利用

$$P(E)=\frac{E\text{中元素个数}}{S\text{中元素个数}}=\frac{n(E)}{n(S)}$$

(a) 在 6 种情形中，该事件以 3 种方式(2,4 或 6)出现，因此 $p=\frac{3}{6}=\frac{1}{2}$.

(b) 假设硬币是可区分的，有 8 种情形：

HHH，HHT，HTH，HTT，THH，THT，TTH，TTT，

只有最后一个情形不符合，故 $p=\frac{7}{8}$.

(c) 有 $4+3+5=12$ 个弹子，其中 3 个红弹子. 因此，$p=\frac{3}{12}=\frac{1}{4}$.

7.6 从一副 52 张的普通纸牌 S 中抽出一张. 求其概率.

(a) 这张牌为 K.

(b) 这张牌为大牌(J，Q 或 K).

(c) 这张牌为红心.

(d) 这张牌为红心大牌.

(e) 这张牌为大牌或红心.

解 ☞ 这里 $n(S)=52$.

(a) 有 4 张 K，因此，$p=\frac{4}{52}=\frac{1}{13}$.

(b) 有 $4\times3=12$ 张大牌. 因此，$p=\frac{12}{52}=\frac{3}{13}$.

(c) 有 13 张红心，因此，$p=\frac{13}{52}=\frac{1}{4}$.

(d) 有 3 张红心大牌. 因此，$p=\frac{3}{52}$.

(e) 设 $F=\{\text{大牌}\}$，$H=\{\text{红心}\}$，则

$$n(F\cup H)=n(F)+n(H)-n(F\cap H)=12+13-3=22.$$

因此，$p=\frac{22}{52}=\frac{11}{26}$.

7.7 考虑问题 7.2 中的样本空间 S. 假设硬币与骰子是公正的. 因此 S 为等概率空间. 求：

(a) $P(A)$，$P(B)$，$P(C)$；　　(b) $P(A\cup B)$，$P(B\cap C)$，$P(B\cap A^c\cap C^c)$.

解 ☞ 由于 S 为等概率空间，所以利用 $P(E)=\frac{n(E)}{n(S)}$. 这里 $n(S)=12$. 只需计数给定集中元素的个数.

(a) $P(A)=\frac{3}{12}$，$P(B)=\frac{6}{12}$，$P(C)=\frac{3}{12}$，

(b) $P(A\cup B)=\frac{8}{12}$，$P(B\cap C)=\frac{2}{12}$，$P(B\cap A^c\cap C^c)=\frac{3}{12}$.

7.8　随机地从一副 52 张的普通纸牌中抽取两种纸牌. 求其概率：

(a) 两张是黑桃；　(b) 一张黑桃，一张红心.

解 ☞　从 52 张中抽取 2 张有 $\binom{52}{2}=1326$ 种方法.

(a) 从 13 张黑桃中抽取两张黑桃有 $\binom{13}{2}=78$ 种方法. 由此，

$$p=\frac{\text{抽取 2 张黑桃的方法数}}{\text{抽取 2 张牌的方法数}}=\frac{78}{1326}=\frac{3}{51}.$$

(b) 有 13 张黑桃与 13 张红心. 因此有 $13\cdot 13=169$ 种方法抽取一张黑桃和一张红心. 由此 $p=\frac{169}{1326}=\frac{13}{102}$.

7.9　一个盒子装有两只白袜子和两只蓝袜子. 随机地取出两只袜子. 求它们是相配的(同色的)概率.

解 ☞　有 $\binom{4}{2}=6$ 种方法取两只袜子，只有两双是相配的. 于是 $p=\frac{2}{6}=\frac{1}{3}$.

7.10　5 匹马参加比赛、Audrey 随机地选择两匹马，并赌它们会胜. 求 Audrey 选出获胜马的概率 p.

解 ☞　有 $\binom{5}{2}=10$ 种方法选取两匹马. 其中 4 对将包含获胜马. 因此 $p=\frac{4}{10}=\frac{2}{5}$.

有限概率空间

7.11　样本空间 S 有 4 个元素，即 $S=\{a_1,a_2,a_3,a_4\}$. S 在下列哪个函数下成为概率空间?

(a) $P(a_1)=\frac{1}{2}$，　$P(a_2)=\frac{1}{3}$，　$P(a_3)=\frac{1}{4}$，　$P(a_4)=\frac{1}{5}$.

(b) $P(a_1)=\frac{1}{2}$，　$P(a_2)=\frac{1}{4}$，　$P(a_3)=-\frac{1}{4}$，　$P(a_4)=\frac{1}{2}$.

(c) $P(a_1)=\frac{1}{2}$，　$P(a_2)=\frac{1}{4}$，　$P(a_3)=\frac{1}{8}$，　$P(a_4)=\frac{1}{8}$.

(d) $P(a_1)=\frac{1}{2}$，　$P(a_2)=\frac{1}{4}$，　$P(a_3)=\frac{1}{4}$，　$P(a_4)=0$.

解 ☞　(a) 由于样本点值的和大于 1，所以这个函数未将 S 定义为概率空间.

(b) 由于 $P(a_3)$ 为负数. 所以这个函数未将 S 定义为概率空间.

(c) 由于每个值是非负的，且它们的和为 1，所以这个函数定义 S 为一个概率空间.

(d) 所有值都是非负的，且相加为 1，因此该函数将 S 定义为一个概率空间.

7.12　加重一枚硬币，使得正面朝上的可能性为反面朝上的两倍. 求 $P(T)$ 和 $P(H)$.

解 ☞　设 $P(T)=p$，则 $P(H)=2p$. 令概率的和等于 1. 即令 $p+2p=1$. 于是 $p=\frac{1}{3}$. 因此 $P(H)=\frac{2}{3}$，$P(T)=\frac{1}{3}$.

7.13　加重一个骰子使得结果给出下面的概率分布：

结　果	1	2	3	4	5	6
概　率	0.1	0.3	0.2	0.1	0.1	0.2

考虑事件：

$$A=\{\text{偶数}\},\quad B=\{2,3,4,5\},\quad C=\{x : x<3\},\quad D=\{x : x>7\}.$$

求下列概率：

(a)　(i) $P(A)$，　(ii) $P(B)$，　(iii) $P(C)$，　(iv) $P(D)$.

(b)　$P(A^c)$，$P(B^c)$，$P(C^c)$，$P(D^c)$.

(c)　(i) $P(A\cap B)$，　(ii) $P(A\cup C)$，　(iii) $P(B\cap C)$.

解☞　(a) 对任一事件，相加 E 中元素的概率求得 $P(E)$. 因此：

(i) $A=\{2,4,6\}$，因此 $P(A)=0.3+0.1+0.2=0.6$.

(ii) $P(B)=0.3+0.2+0.1+0.1=0.7$.

(iii) $C=\{1,2\}$，因此 $P(C)=0.1+0.3=0.4$.

(iv) $D=\varnothing$，空集. 因此 $P(D)=0$.

(b) 利用 $P(E^c)=1-P(E)$ 可得

$$P(A^c)=1-0.6=0.4,\qquad P(C^c)=1-0.4=0.6,$$
$$P(B^c)=1-0.7=0.3,\qquad P(D^c)=1-0=1.$$

(c) (i) $A\cap B=\{2,4\}$，因此 $P(A\cap B)=0.3+0.1=0.4$.

(ii) $A\cup C=\{1,2,3,4,5\}=\{6\}^c$，因此 $P(A\cup C)=1-0.2=0.8$.

(iii) $B\cap C=\{2\}$，因此 $P(B\cap C)=0.3$.

7.14　设 A,B 为两个事件，且 $P(A)=0.6$，$P(B)=0.3$，$P(A\cap B)=0.2$. 求概率：

(a) A 不发生.　　　(b) B 不发生.

(c) A 或 B 发生.　　(d) A,B 都不发生.

解☞　(a) $P(\text{非 }A)=P(A^c)=1-P(A)=0.4$.

(b) $P(\text{非 }B)=P(B^c)=1-P(B)=0.7$.

(c) 由加法原理，得

$$P(A\text{ 或 }B)=P(A\cup B)=P(A)+P(B)-P(A\cap B)$$
$$=0.6+0.3-0.2=0.7.$$

(d) 回忆(图 7-3(b)) A,B 都不发生就是 $A\cup B$ 的补. 因此

$$P(A,B\text{ 都不发生})=P((A\cup B)^c)=1-P(A\cup B)=1-0.7=0.3.$$

7.15　证明定理 7.2：$P(A^c)=1-P(A)$.

证☞　$S=A\cup A^c$，A 与 A^c 是不交的. 于是

$$1=P(S)=P(A\cup A^c)=P(A)+P(A^c).$$

由此得证.

7.16　证明定理 7.3：

(i) $P(\varnothing)=0$，

(ii) $P(A\backslash B)=P(A)-P(A\cap B)$，

(iii) 若 $A\subseteq B$，则 $P(A)\leqslant P(B)$.

证☞　(i) $\varnothing=S^c$，且 $P(S)=1$. 因此 $P(\varnothing)=1-1=0$.

(ii) 正如图 7-5(a)，$A=(A\backslash B)\cup(A\cap B)$，$A\backslash B$ 与 $A\cap B$ 不相交，因此

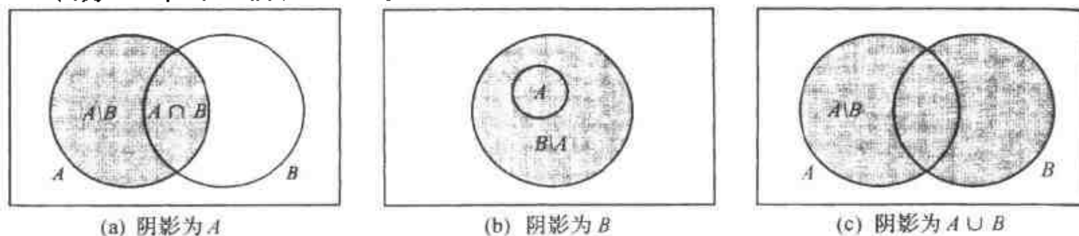
$$P(A)=P(A\backslash B)+P(A\cap B).$$

由此得证.

(iii) 若 $A\subseteq B$. 则，如图 7-5(b)，$B=A\cup(B\backslash A)$，这里 A 与 $B\backslash A$ 是不相交的，因此，

$$P(B)=P(A)+P(B\backslash A).$$

因为 $P(B\backslash A)\geqslant 0$，所以 $P(A)\leqslant P(B)$.



(a) 阴影为 A　　(b) 阴影为 B　　(c) 阴影为 $A\cup B$

图 7-5

7.17 证明定理7.4(加法原理):对任何事件 A 和 B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

证 ☞ 如图7-5(c)所示,$A \cup B = (A \backslash B) \cup B$.这里 $A \backslash B$ 与 B 互不相交.于是,利用定理7.3(ii)得,

$$\begin{aligned} P(A \cup B) &= P(A \backslash B) + P(B) = P(A) - P(A \cap B) + P(B) \\ &= P(A) + P(B) - P(A \cap B). \end{aligned}$$

条件概率

7.18 3枚硬币,一分,伍分和一角各掷一次.如果(a) 一分正面朝上;(b) 至少一枚硬币正面朝上,求都是正面朝上的概率 p.

样本空间有8个元素:

$$S = \{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT\}.$$

解 ☞ (a) 若一分币正面朝上,则诱导样本空间为

$$A = \{HHH, HHT, HTH, HTT\}.$$

因为所有硬币都正面朝上在四种情形中只有一种符合.所以 $p = \frac{1}{4}$.

(b) 若一个或多个正面朝上,则诱导样本空间为

$$B = \{HHH, HHT, HTH, HTT, THH, THT, TTH\}.$$

由于所有硬币都正面朝上在7种情形只有一个符合.所以 $p = \frac{1}{7}$.

7.19 抛一对骰子.如果(a) 第一个骰子出现5;(b) 至少一个骰子出现5.求和大于或等于10的概率.

解 ☞ (a) 若第1个骰子出现5,则诱导样本空间为

$$A = \{(5,1), (5,2), (5,3), (5,4), (5,5), (5,6)\}.$$

和大于或等于10在6个结果中有2个:(5,5),(5,6).因此 $p = \frac{2}{6} = \frac{1}{3}$.

(b) 若至少一个骰子出现5,则诱导样本空间有11个元素.

$$\begin{aligned} B = \{&(5,1), (5,2), (5,3), (5,4), (5,5), (5,6), \\ &(1,5), (2,5), (3,5), (4,5), (6,5)\}. \end{aligned}$$

和大于或等于10在11个结果中有3个:(5,5),(5,6)和(6,5).因此 $p = \frac{3}{11}$.

7.20 在某大学城,25%的学生数学不及格,15%的学生化学不及格,10%的学生数学与化学两门不及格.现随机地选一个学生.

(a) 若他化学不及格,则他数学不及格的概率是多少?

(b) 若数学不及格,则他化学不及格的概率是多少?

(c) 他数学或化学不及格的概率是多少?

(d) 他数学与化学都没有不及格的概率是多少?

解 ☞ (a) 已知该生化学不及格,则他数学不及格的概率为

$$P(M \mid C) = \frac{P(M \cap C)}{P(C)} = \frac{0.10}{0.15} = \frac{2}{3}.$$

(b) 已知该生数学不及格,则他化学不及格的概率为

$$P(C \mid M) = \frac{P(C \cap M)}{P(M)} = \frac{0.10}{0.25} = \frac{2}{5}.$$

(c) 由加法原理(定理7.4),

$$P(M \cup C) = P(M) + P(C) - P(M \cap C) = 0.25 + 0.15 - 0.10 = 0.30.$$

(d) 数学和化学都没有不及格的学生为集合 $M \cup C$ 的补,即为集合 $(M \cup C)^c$.因此,

$$P((M \cup C)^c) = 1 - P(M \cup C) = 1 - 0.30 = 0.70.$$

7.21 抛一对骰子.若出现的两数不同,求概率:(a) 和为6;(b) 出现一个幺点;(c) 和不超过4.

解 ☞ 有36种方法抛一对骰子.其中有6个:(1,1),(2,2),…,(6,6)有相同的数.于是诱导样本空

间有 36－6＝30 个元素.

(a) 和为 6 有 4 种方式出现：(1,5),(2,4),(4,2),(5,1).(不包括(3,3),因为这两个数相同.)因此，

$p=\frac{4}{30}=\frac{2}{15}$.

(b) 出现幺点有 10 种方式：(1,2),(1,3),…,(1,6)和(2,1),(3,1),…,(6,1).因此 $p=\frac{10}{30}=\frac{1}{3}$.

(c) 和不超过 4 有 4 种方式：(3,1),(1,3),(2,1),(1,2).因此，$p=\frac{4}{30}=\frac{2}{15}$.

7.22 一个班有 12 名男生和 4 名女生.若随机地从中选取 3 名学生,求都是男生的概率.

解 选出的第一名是男生的概率为$\frac{12}{16}$,因为 16 名学生中有 12 位男生.若第一位是男生,则第二位是男生的概率为$\frac{11}{15}$,因为剩下的 15 名学生中有 11 位男生.最后,若前两位是男生,则第三位是男生的概率为$\frac{10}{14}$,因为剩下的 14 名学生中有 10 名男生.因此,由乘法原理,3 名都是男生的概率为

$$p=\frac{12}{16}\cdot\frac{11}{15}\cdot\frac{10}{14}=\frac{11}{28}.$$

另解 有 $C(16,3)=560$ 种方法从 16 名学生中选 3 位且有 $C(12,3)=220$ 种方法从 12 名男生中选 3 名男生.因此 $p=\frac{220}{560}=\frac{11}{28}$.

又解 若一个一个地选,则有 16·15·14 种方法选 3 名学生.有 12·11·10 种方法选 3 名男学生.因此

$$p=\frac{12\cdot 11\cdot 10}{16\cdot 15\cdot 14}=\frac{11}{28}.$$

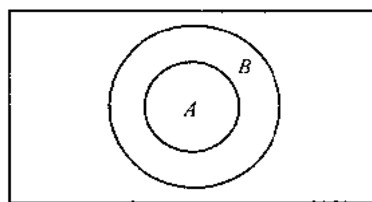
7.23 设 $P(A)>0$,若(a) A 为 B 的子集;(b) A 与 B 相互排斥.则求 $P(B|A)$.

解 (a) 若 A 为 B 的子集(如图 7－6(a)),则 A 发生 B 一定发生.因此 $P(B|A)=1$.或,若 A 为 B 的子集,则 $A\cap B=A$.因此,

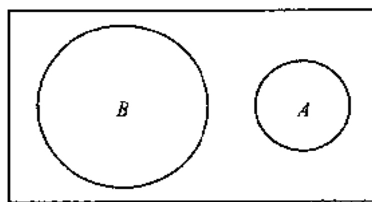
$$P(B|A)=\frac{P(A\cap B)}{P(A)}=\frac{P(A)}{P(A)}=1.$$

(b) 若 A 与 B 相互排斥,即不相交(如图 7－6(b)).则 A 发生 B 一定不发生.因此 $P(B|A)=0$.或,若 A 与 B 不相交,则 $A\cap B=\varnothing$,因此

$$P(B|A)=\frac{P(A\cap B)}{P(A)}=\frac{P(\varnothing)}{P(A)}=\frac{0}{P(A)}=0.$$



(a) $A\subseteq B$



(b) $A\cap B=\varnothing$

图 7－6

独立性

7.24 A 击中目标的概率为$\frac{1}{3}$,B 击中目标的概率为$\frac{1}{5}$.他们都向目标射击.求其概率:(a) A 未击中目标;(b) 都击中目标;(c) 一人击中目标;(d) 没有人击中目标.

解 已知 $P(A)=\frac{1}{3}$,$P(B)=\frac{1}{5}$(假设事件是独立的).

(a) $P(\text{非}A)=P(A^c)=1-P(A)=1-\frac{1}{3}=\frac{2}{3}$.

(b) 由于事件是独立的,所以

$P(A\text{与}B)=P(A\cap B)=P(A)P(B)=\frac{1}{3}\cdot\frac{1}{5}=\frac{1}{15}$.

(c) 由加法原理(定理 7.4),

$$P(A\text{或}B)=P(A\cup B)=P(A)+P(B)-P(A\cap B)=\frac{1}{3}+\frac{1}{5}-\frac{1}{15}=\frac{7}{15}.$$

(d) $P(\text{既非}A\text{也非}B)=P((A\cup B)^c)=1-P(A\cup B)=1-\frac{7}{15}=\frac{8}{15}$.

7.25 对一个有子女的家庭考虑以下事件:

$$A=\{\text{有男有女}\}, \qquad B=\{\text{至多一个男孩}\}.$$

(a) 若该家庭有三名子女,则 A 与 B 独立.

(b) 若只有两名子女,则 A 与 B 相关.

解 ☞ (a) 等概率空间为 $S=\{bbb,bbg,bgb,bgg,gbb,gbg,ggb,ggg\}$. 因此,

$A=\{bbg,bgb,bgg,gbb,gbg,ggb\}$,由此, $P(A)=\frac{6}{8}=\frac{3}{4}$,

$B=\{bgg,gbg,ggb,ggg\}$, 由此, $P(B)=\frac{4}{8}=\frac{1}{2}$,

$A\cap B=\{bgg,gbg,ggb\}$, 由此, $P(A\cap B)=\frac{3}{8}$,

因为 $P(A)P(B)=\frac{3}{4}\cdot\frac{1}{2}=\frac{3}{8}=P(A\cap B)$,所以 A 与 B 独立.

(b) 等概率空间 $S=\{bb,bg,gb,gg\}$,因此

$A=\{bg,gb\}$, 由此, $P(A)=\frac{1}{2}$,

$B=\{bg,gb,gg\}$,由此, $P(B)=\frac{3}{4}$,

$A\cap B=\{bg,gb\}$,由此, $P(A\cap B)=\frac{1}{2}$.

由于 $P(A)P(B)\neq P(A\cap B)$,所以 A 与 B 相关.

7.26 A 盒装有 5 个红弹子和 3 个蓝弹子,B 盒装有 3 个红弹子和 2 个蓝弹子. 随机地从每个盒子中取一个弹子.

(a) 求两个弹子都是红色的概率.

(b) 求一个红色一个蓝色的概率.

解 ☞ (a) 从 A 盒中选一个红弹子的概率为$\frac{5}{8}$,从 B 盒中选一个红弹子的概率为$\frac{3}{5}$. 因为事件是独立的,所以 $p=\frac{5}{8}\cdot\frac{3}{5}=\frac{3}{8}$.

(b) 从 A 中选一个红弹子,从 B 中选一个蓝弹子的概率 p_1 为$\frac{5}{8}\cdot\frac{2}{5}=\frac{1}{4}$;从 A 中选一个蓝弹子,从 B 中选一个红弹子的概率 $p_2=\frac{3}{8}\cdot\frac{3}{5}=\frac{9}{40}$. 因此 $p=p_1+p_2=\frac{1}{4}+\frac{9}{40}=\frac{19}{40}$.

7.27 证明:若 A,B 为独立事件,则 A^c 与 B^c 是独立事件.

证 ☞ 设 $P(A)=x,P(B)=y$,则 $P(A^c)=1-x,P(B^c)=1-y$. 由于 A,B 为独立的,所以 $P(A\cap B)=P(A)P(B)=xy$. 此外,

$$P(A\cup B)=P(A)+P(B)-P(A\cap B)=x+y-xy.$$

由 DeMorgan 定律,$(A\cup B)^c=A^c\cap B^c$. 因此

$$P(A^c\cap B^c)=P((A\cup B)^c)=1-P(A\cup B)=1-x-y+xy.$$

另一方面,

$$P(A^c)P(B^c)=(1-x)(1-y)=1-x-y+xy.$$

于是 $P(A^c\cap B^c)=P(A^c)P(B^c)$,由此,$A^c$ 与 B^c 独立.

类似地可以证明 A 与 B^c,A^c 与 B 都是独立的.

重复试验,二项分布

7.28 4 匹马 a,b,c,d 一同比赛. 它们各自的获胜概率分别为 0.2,0.5,0.1,0.2,即 $S=$

$\{a,b,c,d\}$，$P(a)=0.2$，$P(b)=0.5$，$P(c)=0.1$，$P(d)=0.2$. 现比赛 3 次.

(a) 描述并求积概率空间 S_3 中元素的个数.

(b) 求同一匹马胜 3 场的概率.

(c) 求 a,b,c 各胜一场的概率.

解 ☞ (a) 由定义，$S_3=S\times S\times S=\{(x,y,z): x,y,z\in S\}$，且

$$P((x,y,z)) = P(x)P(y)P(z).$$

于是，特别地，S_3 含有 $4^3=64$ 个元素.

(b) 记(x,y,z)为 xyz. 求事件 $A=\{aaa,bbb,ccc\}$的概率. 由定义

$$P(aaa)=(0.2)^3=0.008,\quad P(ccc)=(0.1)^3=0.001,$$

$$P(bbb)=(0.5)^3=0.125,\quad P(ddd)=(0.2)^3=0.008,$$

于是，

$$P(A)=0.008+0.125+0.001+0.008=0.142.$$

(c) 求事件 $B=\{abc,acb,bac,bca,cab,cba\}$的概率. B 中的每个事件有相同的概率.

$$0.2\times 0.5\times 0.1=0.01.$$

因此 $P(B)=6\times 0.01=0.06$.

7.29 掷一枚硬币 3 次. 求出现(a) 3 次正面，(b) 恰两次正面；(c) 恰一次正面；(d) 没有正面的概率.

解 ☞ 掷硬币时，用 H 表示正面，T 表示反面，3 次投掷可看成等概率空间，它有 8 种可能的结果：

$$S=\{\text{HHH},\text{HHT},\text{HTH},\text{HTT},\text{THH},\text{THT},\text{TTH},\text{TTT}\}$$

由于任一投掷的结果不依赖于其他投掷的结果，所以 3 次投掷可看成 3 次独立试验，每次试验 $P(H)=\frac{1}{2}$，$P(T)=\frac{1}{2}$. 那么：

(a) $P(3\text{次正面})=P(\text{HHH})=\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{8}$.

(b) $P(\text{恰 2 次正面})=P(\text{HHT,或 HTH,或 THH})$

$$=\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}=\frac{3}{8}.$$

(c) 如(b)，$P(\text{恰一次正面})=P(\text{恰两次反面})=\frac{3}{8}$.

(d) 如(a)，$P(\text{没有正面})=P(3\text{次反面})=\frac{1}{8}$.

7.30 John 击中目标的概率为 $p=\frac{1}{4}$. 他射击 $n=6$ 次. 求他击中目标(a) 恰两次；(b) 多于 4 次；(c) 至少一次的概率.

解 ☞ 这是 $n=6$，$p=\frac{1}{4}$，$q=1-p=\frac{3}{4}$的二项试验，即 $B\left(6,\frac{1}{4}\right)$. 由此，利用定理 7.7.

(a) $P(2)=\binom{6}{2}\left(\frac{1}{4}\right)^2\left(\frac{3}{4}\right)^4=15(3^4)/(4^6)=\frac{1215}{4096}\approx 0.297$.

(b) $P(5)+P(6)=\binom{6}{5}\left(\frac{1}{4}\right)^5\left(\frac{3}{4}\right)^1+\left(\frac{1}{4}\right)^6=\frac{18^6}{4^6}+\frac{1^6}{4^6}=\frac{19^6}{4^6}=\frac{19}{4096}\approx 0.0046$.

(c) $P(0)=\left(\frac{3}{4}\right)^6=\frac{729}{4096}$，因此，$P(X>0)=1-\frac{729}{4096}=\frac{3367}{4096}\approx 0.82$.

7.31 假设某厂生产的产品 20%为次品. 设随机地选取 4 件. 求概率：(a) 两件次品；(b) 三件次品；(c) 没有次品.

解 ☞ 这是 $n=4$，$p=0.2$，$q=1-p=0.8$ 的二项试验，即 $B(4,0.2)$. 因此，由定理 7.7 得，

(a) $P(2)=\binom{4}{2}(0.2)^2(0.8)^2=0.1536$.

(b) $P(3)=\binom{4}{3}(0.2)^3(0.8)^1=0.0256$.

(c) $P(0)=(0.8)^4=0.4096$.

7.32 A 参加比赛时获胜的概率为$\frac{2}{3}$. 设 A 打 4 场比赛. 求 A 获胜超过半数的概率.

解 这里 $n=4, p=\frac{2}{3}, q=1-p=\frac{1}{3}$. 若 A 获胜 3 场或 4 场比赛,则 A 获胜超过半数. 因此,

$$p=P(3)+P(4)=\binom{4}{3}\left(\frac{2}{3}\right)^3\left(\frac{1}{3}\right)^1+\binom{4}{4}\left(\frac{2}{3}\right)^4=\frac{32}{81}+\frac{16}{81}=\frac{16}{27}=0.59.$$

7.33 某家庭有 6 个子女. 求有

(a) 三男三女; (b) 男孩少于女孩

的概率. 假设任一小孩为男孩的概率为$\frac{1}{2}$.

解 这里 $n=6, p=q=\frac{1}{2}$.

(a) $p=P(\text{三男})=\binom{6}{3}\left(\frac{1}{2}\right)^3\left(\frac{1}{2}\right)^3=\frac{20}{64}=\frac{5}{16}$.

(b) 若没有,有一个,或有两个男孩,则男孩比女孩少. 因此

$$\begin{aligned}p&=P(\text{没有男孩})+P(\text{一个男孩})+P(2\text{ 个男孩})\\&=\left(\frac{1}{2}\right)^6+\binom{6}{1}\left(\frac{1}{2}\right)^5\frac{1}{2}+\binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4=\frac{11}{32}=0.34.\end{aligned}$$

7.34 某种导弹以 $p=0.3$ 的概率击中目标. 为达到至少 80%的概率击中目标,至少应发射多少枚导弹.

解 未击中目标的概率为 $q=1-p=0.7$. 因此 n 枚导弹未击中目标的概率为 0.7^n. 于是求最小的 n 使得

$$1-0.7^n>0.8.$$

即

$$0.7^n<0.2.$$

计算:$0.7^1=0.7$, $0.7^2=0.49$, $0.7^3=0.343$, $0.7^4=0.2401$, $0.7^5=0.16807$.

因此,至少应发射 5 枚导弹.

7.35 至少应掷骰子多少个,才能使得获得 6 的机会更大?

解 对 n 个骰子,不能得到 6 的概率为$\left(\frac{5}{6}\right)^n$. 因此,求最小的 n,使得

$$\left(\frac{5}{6}\right)^n<\frac{1}{2}.$$

计算:$\left(\frac{5}{6}\right)^1=\frac{5}{6}$, $\left(\frac{5}{6}\right)^2=\frac{25}{36}$, $\left(\frac{5}{6}\right)^3=\frac{125}{216}$,但$\left(\frac{5}{6}\right)^4=\frac{625}{1296}<\frac{1}{2}$. 因此必须投掷 4 个骰子.

7.36 某足球队获胜(W)概率为 0.6,输球(L)概率为 0.3,平局(T)概率为 0.1. 该队在周末打 3 场比赛. (a) 确定该队至少胜两场且一场未输事件 A 的元素,并求 $P(A)$.

(b) 确定该队按某顺序胜、输、平的事件 B 的元素,并求 $P(B)$.

解 (a) A 由至少有 2 个 W,没有 L 的所有三元有序组构成. 于是

$$A=\{\text{WWW},\text{WWT},\text{WTW},\text{TWW}\}.$$

进一步,

$$\begin{aligned}P(A)&=P(\text{WWW})+P(\text{WWT})+P(\text{WTW})+P(\text{TWW})\\&=(0.6)(0.6)(0.6)+(0.6)(0.6)(0.1)\\&\quad+(0.6)(0.1)(0.6)+(0.1)(0.6)(0.6)\\&=0.216+0.036+0.036+0.036=0.324.\end{aligned}$$

(b) $B=\{\text{WLT},\text{WTL},\text{LWT},\text{LTW},\text{TWL},\text{TLW}\}$. B 中的每个元素的概率为$(0.6)\cdot(0.3)\cdot(0.1)=0.018$. 因此,

$$P(B)=6\times0.018=0.108.$$

7.37 某人向目标开火 $n=6$ 次,击中目标 $k=2$ 次.

(a) 列出各种可能情形.

(b) 共有多少种情形?

解 (a) 列出全部有两次成功(S)和4次失败(F)的序列:

SSFFFF, SFSFFF, SFFSFF, SFFFSF, SFFFFS, FSSFFF, FSFSFF, FSFFSF, FSFFFS, FFSSFF, FFSFSF, FFSFFS, FFFSSF, FFFSFS, FFFFSS

(b) 上面列出了15种不同的情形. 注意这等于$\binom{6}{2}$. 因为我们在序列的$n=6$个位置分配两个字母S.

7.38 证明定理7.7:二项试验$B(n,p)$中恰k次成功的概率为

$$P(k) = P(k\text{ 次成功}) = \binom{n}{k}p^k q^{n-k}.$$

一次或更多次成功的概率为$1-q^n$.

证 n个重复试验的样本空间由所有分量为S(成功)或F(失败)的n-元组(n-元序列)构成. 设A为恰k次成功的事件. 则A由k个分量为S, $n-k$个分量为F的所有n-元组构成. 事件A中的n-元组的个数等于在n-元组的n个分量中分配k个字母S的方法数,因此,A含$C(n,k)=\binom{n}{k}$个样本点. A中每个点的概率为$p^k q^{n-k}$,因此,

$$P(A) = \binom{n}{k}p^k q^{n-k}.$$

特别地,没有成功的概率为

$$P(0) = \binom{n}{0}p^0 q^n = q^n.$$

因此,一次或多次成功的概率为$1-q^n$.

随机变量,期望

7.39 一位选手掷两枚硬币,若两个正面,则他赢2美元,若一个正面,则赢1美元. 另一方面,若没有正面,则他输3美元. 求比赛的期望值E. 比赛公平否?

(根据$E=0$, $E>0$或$E<0$,比赛对选手公平、有利或不利.)

解 样本空间$S=\{HH,HT,TH,TT\}$,且每个样本点概率为$\frac{1}{4}$. 根据选手所得,有

$$X(HH)=2,\qquad X(HT)=X(TH)=1,\qquad X(TT)=-3$$

因此,X的分布为

x_i	2	1	−3
p_i	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{1}{4}$

且

$$E=E(X)=2\left(\frac{1}{4}\right)+1\left(\frac{2}{4}\right)-3\left(\frac{1}{4}\right)=0.25.$$

因为$E(X)>0$,所以比赛对选手有利.

7.40 随机地从1到3中选两个数,允许重复. 设X为两数之和. (a) 求X的分布. (b) 求期望$E(X)$.

解 (a) 有9个等可能的数对构成了样本空间S. X假设值2,3,4,5,6具有下面的概率:

$$P(2)=P(1,1)=\frac{1}{9},\qquad P(3)=P(\{(1,2),(2,1)\})=\frac{2}{9},$$

$$P(4)=P(\{(1,3),(2,2),(3,1)\})=\frac{3}{9},$$

$$P(5)=P(\{(2,3),(3,2)\})=\frac{2}{9},\qquad P(6)=P(3,3)=\frac{1}{9}.$$

因此,分布为

x_i	2	3	4	5	6
$P(x_i)$	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{3}{9}$	$\frac{2}{9}$	$\frac{1}{9}$

(b) 用 x 的值乘以其概率再相加可得期望值 $E(X)$. 因此

$$E(X)=2\left(\frac{1}{9}\right)+3\left(\frac{2}{9}\right)+4\left(\frac{3}{9}\right)-5\left(\frac{2}{9}\right)+6\left(\frac{1}{9}\right)=\frac{36}{9}=4.$$

7.41 加重一枚硬币使得 $P(\mathrm{H})=\frac{3}{4}$, $P(\mathrm{T})=\frac{1}{4}$. 现投掷硬币 3 次. 设 X 表示正面朝上的次数. (a) 求 X 的分布. (b) 求期望 $E(X)$.

解☞ (a) 样本空间为

$$S=\{\mathrm{HHH},\mathrm{HHT},\mathrm{HTH},\mathrm{HTT},\mathrm{THH},\mathrm{THT},\mathrm{TTH},\mathrm{TTT}\}.$$

X 假设值 0,1,2,3 的概率为

$$P(0)=P(\mathrm{TTT})=\frac{1}{4}\cdot\frac{1}{4}\cdot\frac{1}{4}=\frac{1}{64},$$

$$P(1)=P(\mathrm{HTT},\mathrm{THT},\mathrm{TTH})$$
$$=\frac{3}{4}\cdot\frac{1}{4}\cdot\frac{1}{4}+\frac{1}{4}\cdot\frac{3}{4}\cdot\frac{1}{4}+\frac{1}{4}\cdot\frac{1}{4}\cdot\frac{3}{4}=\frac{9}{64},$$

$$P(2)=P(\mathrm{HHT},\mathrm{HTH},\mathrm{THH})$$
$$=\frac{3}{4}\cdot\frac{3}{4}\cdot\frac{1}{4}+\frac{3}{4}\cdot\frac{1}{4}\cdot\frac{3}{4}+\frac{1}{4}\cdot\frac{3}{4}\cdot\frac{3}{4}=\frac{27}{64},$$

$$P(3)=P(\mathrm{HHH})=\frac{3}{4}\cdot\frac{3}{4}\cdot\frac{3}{4}=\frac{27}{64}.$$

因此,分布为

x_i	0	1	2	3
$P(x_i)$	$\frac{1}{64}$	$\frac{9}{64}$	$\frac{27}{64}$	$\frac{27}{64}$

(b) 用 x 的每个值乘以其概率再求和求得期望值 $E(X)$. 因此

$$E(X)=0\left(\frac{1}{64}\right)+1\left(\frac{9}{64}\right)-2\left(\frac{27}{64}\right)+3\left(\frac{27}{64}\right)=\frac{144}{64}=2.25.$$

7.42 你在某竞赛中获胜. 奖励从 3 个密封的信封中选取. 已知有两个信封每个含 30 美元的支票. 但另一个信封含 3000 美元的支票. 你的奖金(作为概率分布)的期望值 E 是多少?

解☞ 设 X 表示你的奖金,则 $X=30$ 或 3000. 且 $P(30)=\frac{2}{3}$, $P(3000)=\frac{1}{3}$. 因此

$$E=E(X)=30\cdot\frac{2}{3}+3000\cdot\frac{1}{3}=20+1000=1020.$$

7.43 掷一枚硬币直至出现一次正面或五次反面. 求硬币投掷的期望值 E.

解☞ 可能的结果为

$$\mathrm{H},\mathrm{TH},\mathrm{TTH},\mathrm{TTTH},\mathrm{TTTTH},\mathrm{TTTTT}$$

各自的概率(独立试验)为

$$\frac{1}{2},\quad\left(\frac{1}{2}\right)^2=\frac{1}{4},\quad\left(\frac{1}{2}\right)^3=\frac{1}{8},\quad\left(\frac{1}{2}\right)^4=\frac{1}{16},$$

$$\left(\frac{1}{2}\right)^5=\frac{1}{32},\quad\left(\frac{1}{2}\right)^5=\frac{1}{32}$$

有趣的是,随机变量 X 就是各自结果中投掷的次数. 于是

$$X(\mathrm{H})=1,\qquad X(\mathrm{TTH})=3,\qquad X(\mathrm{TTTTH})=5,$$
$$X(\mathrm{TH})=2,\qquad X(\mathrm{TTTH})=4,\qquad X(\mathrm{TTTTT})=5.$$

且这些 X 的值有概率:

$$P(1)=P(\mathrm{H})=\frac{1}{2},\qquad P(2)=P(\mathrm{TH})=\frac{1}{4},$$

$$P(3)=P(\mathrm{TTH})=\frac{1}{8},\quad P(4)=P(\mathrm{TTTH})=\frac{1}{16},$$

$$P(5)=P(\mathrm{TTTTH})+P(\mathrm{TTTTT})=\frac{1}{32}+\frac{1}{32}=\frac{1}{16}.$$

因此，

$$E=E(X)=1\cdot\frac{1}{2}+2\cdot\frac{1}{4}+3\cdot\frac{1}{8}+4\cdot\frac{1}{16}+5\cdot\frac{1}{16}\approx 1.9$$

7.44 一个线性组 EMPLOYEE 有 n 个元素. 并设 NAME 随机地出现在该组中. 有一个线性查找求出 NAME 的位置 K，即求出 K，使得 EMPLOYEE[K]=NAME. 设 $f(n)$ 表示该线性查找中比较的次数.

(a) 求 $f(n)$ 的期望值.

(b) 求 $f(n)$ 的最大值(最坏情形).

解 (a) 设 X 表示比较的次数. 因为 NAME 以相等的概率 $\frac{1}{n}$ 出现在该组的任一位置. 所以，$X=1,2,\cdots,n$，且每个概率都为 $\frac{1}{n}$. 因此.

$$f(n)=E(X)=1\cdot\frac{1}{n}+2\cdot\frac{1}{n}+3\cdot\frac{1}{n}+\cdots+n\cdot\frac{1}{n}$$

$$=(1+2+\cdots+n)\cdot\frac{1}{n}=\frac{n(n+1)}{2}\cdot\frac{1}{n}=\frac{n+1}{2}.$$

(b) 若 NAME 出现在该组的最后，则 $f(n)=n$.

均值，方差与标准差

7.45 求每个分布的均值 $\mu=E(X)$，方差 $\sigma^2=\mathrm{Var}(X)$ 及标准差 $\sigma=\sigma_X$.

(a)

x_i	2	3	11
p_i	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{6}$

(b)

x_i	1	3	4	5
p_i	0.4	0.1	0.2	0.3

解 使用公式

$$\mu=E(X)=x_1p_1+x_2p_2+\cdots+x_mp_m=\sum x_ip_i,$$

$$\sigma^2=\mathrm{Var}(X)=E(X^2)-\mu^2,$$

$$E(X^2)=x_1^2p_1+x_2^2p_2+\cdots+x_m^2p_m=\sum x_i^2p_i,$$

$$\sigma=\sigma_X=\sqrt{\mathrm{Var}(X)}.$$

(a) $\mu=\sum x_ip_i=2\left(\frac{1}{3}\right)-3\left(\frac{1}{2}\right)+11\left(\frac{1}{6}\right)=4.$

$E(X^2)=\sum x_i^2p_i=2^2\left(\frac{1}{3}\right)+3^2\left(\frac{1}{2}\right)+11^2\left(\frac{1}{6}\right)=26.$

$\sigma^2=\mathrm{Var}(X)=E(X^2)-\mu^2=26-4^2=10.$

$\sigma=\sqrt{\mathrm{Var}(X)}=\sqrt{10}\approx 3.2.$

(b) $\mu=\sum x_ip_i=1(0.4)+3(0.1)+4(0.2)+5(0.3)=3.$

$E(X^2)=\sum x_i^2p_i=1(0.4)+9(0.1)+16(0.2)+25(0.3)=12.$

$\sigma^2 = \text{Var}(X) = E(X^2) - \mu^2 = 12 - 9 = 3.$

$\sigma = \sqrt{\text{Var}(X)} = \sqrt{3} \approx 1.7.$

7.46 5张分别标有1至5的卡片.随机地取两张.用X表示抽出的两数之和.

(a) 求X的分布.

(b) 求X的均值μ,方差$\sigma^2=\text{Var}(X)$和标准差$\sigma=\sigma_X$.

解 (a) 随机地取两张卡片有$C(5,2)=10$种方法.与X的值相对应,有10个等可能的样本点,表示如下:

$$\{1,2\}\to 3,\quad \{1,3\}\to 4,\quad \{1,4\}\to 5,\quad \{1,5\}\to 6,\quad \{2,3\}\to 5,$$

$$\{2,4\}\to 6,\quad \{2,5\}\to 7,\quad \{3,4\}\to 7,\quad \{3,5\}\to 8,\quad \{4,5\}\to 9.$$

注意到X的值有7个数:3,4,5,6,7,8和9.其中3,4,8和9每个有一个样本点,而5,6和7每个有两个样本点.因此,X的分布为

x_i	3	4	5	6	7	8	9
p_i	0.1	0.1	0.2	0.2	0.2	0.1	0.1

(b) $\mu = E(X) = \sum x_i p_i$

$= 3(0.1) + 4(0.1) + 5(0.2) + 6(0.2) + 7(0.2) + 8(0.1) + 9(0.1) = 6.$

$E(X^2) = \sum x_i^2 p_i = 9(0.1) + 16(0.1) + 25(0.2) + 36(0.2) + 49(0.2) + 64(0.1) + 81(0.1) = 39.$

$\text{Var}(X) = E(X^2) - \mu^2 = 39 - 6^2 = 3.$

$\sigma = \sqrt{\text{Var}(X)} = \sqrt{3} \approx 1.7.$

7.47 掷一对骰子.设X表示出现的两数的最大值.

(a) 求X的分布.

(b) 求X的均值μ,方差$\sigma^2=\text{Var}(X)$和标准差$\sigma=\sigma_X$.

解 (a) 由36个整数偶(a,b)构成的样本空间是等概率空间.这里a,b的取值从1到6,即

$$S = \{(1,1),(1,2),\cdots,(6,6)\}.$$

(见问题7.3)由于X将两数中的最大者指派给S中的每个数偶.所以X的值为从1到6的整数.观察得:

(i) 仅一个数偶$(1,1)$给出最大值1,因此$P(1)=\frac{1}{36}$.

(ii) 有3个数偶$(1,2),(2,2),(2,1)$给出最大值2,因此$P(2)=\frac{3}{36}$.

(iii) 5个数偶:$(1,3),(2,3),(3,3),(3,2),(3,1)$给出最大值3.因此$P(3)=\frac{5}{36}$.

类似地,$P(4)=\frac{7}{36}, P(5)=\frac{9}{36}, P(6)=\frac{11}{36}$.

因此,X的分布为

x_i	1	2	3	4	5	6
p_i	$\frac{1}{36}$	$\frac{3}{36}$	$\frac{5}{36}$	$\frac{7}{36}$	$\frac{9}{36}$	$\frac{11}{36}$

(b) 用每个x_i乘以其概率再相加求得X的期望(均值):

$$\mu = E(X) = 1\cdot\frac{1}{36} + 2\cdot\frac{3}{36} + 3\cdot\frac{5}{36} + 4\cdot\frac{7}{36} + 5\cdot\frac{9}{36} + 6\cdot\frac{11}{36}$$

$$= \frac{161}{36} \approx 4.5.$$

用p_i乘以x_i^2,再相加求得$E(X^2)$:

$$E(X^2) = 1\cdot\frac{1}{36} + 4\cdot\frac{3}{36} + 9\cdot\frac{5}{36} + 16\cdot\frac{7}{36} + 25\cdot\frac{9}{36} + 36\cdot\frac{11}{36} = \frac{791}{36} \approx 22.0.$$

因此，

$$\mathrm{Var}(X)=E(X^2)-\mu^2=22.0-(4.5)^2=1.75,$$

$$\sigma_x=\sqrt{1.75}\approx 1.3$$

7.48 投掷一个骰子，设 X 表示出现的数的两倍. 出现奇数时 Y 为 1，出现偶数时 Y 为 3. 求 (a) X；(b) Y 的分布及期望.

解 ☞ 样本空间 $S=\{1,2,3,4,5,6\}$. 每个样本点的概率为 $\frac{1}{6}$.

(a) 样本点的像为

$$X(1)=2,\quad X(2)=4,\quad X(3)=6,$$

$$X(4)=8,\quad X(5)=10,\quad X(6)=12.$$

由于它们都不相同，所以 X 的分布为

x_i	2	4	6	8	10	12
$P(x_i)$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$

于是，

$$E(X)=\sum x_iP(x_i)=\frac{2}{6}+\frac{4}{6}+\frac{6}{6}+\frac{8}{6}+\frac{10}{6}+\frac{12}{6}=7.$$

(b) 样本点的像为

$$Y(1)=1,\quad Y(2)=3,\quad Y(3)=1,$$

$$Y(4)=3,\quad Y(5)=1,\quad Y(6)=3.$$

Y 有 2 个值 1 和 3. 每个在 3 个样本点上取值. 因此 Y 的分布为

y_i	1	3
$P(y_i)$	$\frac{3}{6}$	$\frac{3}{6}$

因此，

$$E(Y)=\sum y_iP(y_i)=\frac{3}{6}+\frac{9}{6}=2.$$

7.49 设 X 和 Y 为定义在同一样本空间 S 上的随机变量，则下面定义的 $Z=X+Y$ 和 $W=XY$ 也为 S 上的随机变量：

$$Z(s)=(X+Y)(s)=X(s)+Y(s),\qquad W(s)=(XY)(s)=X(s)Y(s).$$

设 X 和 Y 为问题 7.48 中的随机变量.

(a) 求 $Z=X+Y$ 的分布与期望，并证明

$$E(X+Y)=E(X)+E(Y).$$

(b) 求 $W=XY$ 的分布与期望.

证 ☞ 样本空间仍为 $S=\{1,2,3,4,5,6\}$. 且每个样本点的概率为 $\frac{1}{6}$.

(a) 利用 $(X+Y)(s)=X(s)+Y(s)$ 及问题 7.48 中 X,Y 的值得到：

$$(X+Y)(1)=2+1=3,\qquad (X+Y)(2)=4+3=7,\qquad (X+Y)(3)=6+1=7,$$

$$(X+Y)(4)=8+3=11,\qquad (X+Y)(5)=10+1=11,\qquad (X+Y)(6)=12+3=15.$$

像的集合为 $\{3,7,11,15\}$. 值 3 和 15 仅在一个样本点得到，因而其概率为 $\frac{1}{6}$；7 和 11在两个样本点得到，因而其概率为 $\frac{2}{6}$. 于是 $Z=X+Y$ 的分布为：

z_i	3	7	11	15
$P(z_i)$	1/6	2/6	2/6	1/6

因此，

$$E(X+Y)=E(Z)=\sum z_iP(z_i)=\frac{3}{6}+\frac{14}{6}+\frac{22}{6}+\frac{15}{6}=9.$$

而且

$$E(X+Y)=9=7+2=E(X)+E(Y).$$

(b) 利用$(XY)(s)=X(s)Y(s)$得到：

$$(XY)(1)=2(1)=2,\qquad (XY)(2)=4(3)=12,\qquad (XY)(3)=6(1)=6,$$
$$(XY)(4)=8(3)=24,\qquad (XY)(5)=10(1)=10,\qquad (XY)(6)=12(3)=36.$$

XY的每个值都恰在一个样本点得到.因此$W=XY$的分布为：

w_i	2	6	10	12	24	36
$P(w_i)$	1/6	1/6	1/6	1/6	1/6	1/6

因此，

$$E(XY)=E(W)=\sum w_iP(w_i)=\frac{2}{6}+\frac{6}{6}+\frac{10}{6}+\frac{12}{6}+\frac{24}{6}+\frac{36}{6}=15.$$

[注意$E(XY)=15\neq(7)(2)=E(X)E(Y)$.]

7.50 某人击中目标的概率为$p=0.1$.他开火100次.求他击中目标的期望值μ,并求标准差σ.

解 ☞ 这是$n=100,p=0.1,q=1-p=0.9$的二项试验$B(n,p)$.因此,由定理7.9得

$$\mu=np=100(0.1)=10,\qquad \sigma=\sqrt{npq}=\sqrt{100(0.1)(0.9)}=3.$$

7.51 某同学做18道多重选择题,每题有4个选择.假设有一个答案是明显不正确的,该同学对剩下的选择作"学过"的猜测.求正确答案的期望值$E(X)$及标准差σ.

解 ☞ 这是$n=18,p=\frac{1}{3},q=1-p=\frac{2}{3}$的二项试验.因此

$$E(X)=np=18\cdot\frac{1}{3}=6,\qquad \sigma=\sqrt{npq}=\sqrt{18\cdot\frac{1}{3}\cdot\frac{2}{3}}=2.$$

7.52 可以证明在样本空间S的随机变量空间上的期望函数$E(X)$是线性的,即

$$E(X_1+X_2+\cdots+X_n)=E(X_1)+E(X_2)+\cdots+E(X_n).$$

利用这个性质证明,对二项试验$B(n,p)$有$\mu=np$.

证 ☞ 在n个Bernoulli试验的样本空间上,记$X_i(i=1,2,\cdots,n)$为随机变量,随机变量根据第i次试验是成功还是失败带有值1或0.那么每个X_i有下面的分布：

x	0	1
$P(x)$	q	p

于是$E(X_i)=0(q)+1(p)=p$. n次试验中成功的总数为

$$X=X_1+X_2+\cdots+X_n.$$

利用E的线性性质,得

$$\begin{aligned}E(X)&=E(X_1+X_2+\cdots+X_n)\\&=E(X_1)+E(X_2)+\cdots+E(X_n)\\&=p+p+\cdots+p=np.\end{aligned}$$

补 充 题

样本空间与事件

7.53 设 A,B 为两个事件. 用集合符号改写下列事件:(a) A 或非 B 发生;(b) 仅 A 发生.

7.54 设 A,B,C 为事件. 用集合符号改写下列事件:(a) A 与 B 但非 C 发生;(b) A 或 C,但非 B 发生;(c) 无一事件发生;(d) 至少两事件发生.

7.55 投掷一枚一分硬币,一枚一角币和一个骰子.

(a) 描述适当的样本空间 S,并求 $n(S)$.

(b) 明确表达下列事件:

$$A=\{\text{两个正面与一个偶数}\},\qquad B=\{\text{出现 }2\},$$
$$C=\{\text{恰好一个正面与一个奇数}\}.$$

(c) 明确表达事件:(i) A 与 B,(ii) 仅 B;(iii) B 与 C.

有限等概率空间

7.56 求每个事件的概率:

(a) 掷一个骰子出现奇数;

(b) 掷 4 个硬币出现一个或更多正面;

(c) 掷两个骰子,一个或两个数都超过 4.

7.57 有 5 名一年级学生,8 名二年级学生,3 名三年级学生和 2 名四年级学生. 现随机地从中选一名学生做代表. 求该学生是(a) 二年级学生,(b) 三年级学生,(c) 三年级或四年级学生的概率.

7.58 随机地从标有 1 到 50 的卡片中选一张卡片. 求卡片上数是(a) 大于 10;(b) 能被 5 整除;(c) 大于 10 且能被 5 整除;(d) 大于 10 或能被 5 整除的数的概率.

7.59 某班 10 个女生中有 3 位蓝眼睛. 随机地选两位女生. 求概率:(a) 都是蓝眼睛;(b) 没有一位是蓝眼睛;(c) 至少一位是蓝眼睛;(d) 恰有一位是蓝眼睛.

7.60 某班有 10 名学生,$A,B,\cdots$. 随机地选三人为班委. 求概率:(a) A 为班委;(b) B 为班委;(c) A 和 B 都是班委;(d) A 或 B 为班委.

7.61 盒中有 3 个螺丝和 3 个螺帽. 随机地取出两件. 求一个为螺丝,另一个为螺帽的概率.

7.62 盒中有两只白袜子,两只蓝袜子和两只红袜子. 随机地取两只袜子. 求它们正好相配(同色)的概率.

7.63 120 名学生中,60 名学法语,50 名学西班牙语,20 名学法语与西班牙语. 随机地选一名学生. 求该生(a) 学法语或西班牙语;(b) 既不学法语也不学西班牙语;(c) 仅学法语;(d) 恰好学两种语言之一的概率.

7.64 3 名男生和 3 名女生随机地坐成一排. 求概率:(a) 3 名女生坐在一起;(b) 男生与女生相间而坐.

有限概率空间

7.65 下列哪个函数使 $S=\{a_1,a_2,a_3\}$ 成为概率空间?

(a) $P(a_1)=\frac{1}{4},P(a_2)=\frac{1}{3},P(a_3)=\frac{1}{2}$.

(b) $P(a_1)=\frac{2}{3},P(a_2)=-\frac{1}{3},P(a_3)=\frac{2}{3}$.

(c) $P(a_1)=\frac{1}{6},P(a_2)=\frac{1}{3},P(a_3)=\frac{1}{2}$.

(d) $P(a_1)=0,P(a_2)=\frac{1}{3},P(a_3)=\frac{2}{3}$.

7.66 加重一枚硬币使得出现正面的概率为出现反面的 3 倍. 求 $P(H)$ 和 $P(T)$.

7.67 3 名同学 A,B,C 进行游泳比赛,A 与 B 有相同的获胜概率,都为 C 获胜概率的 2 倍. 求概率:(a) B 获胜;(b) C 获胜;(c) B 或 C 获胜.

7.68 考察下列概率分布

结果	1	2	3	4	5	6
概率	0.1	0.4	0.1	0.1	0.2	0.1

求下列概率：(a) $P(A)$，$P(B)$，$P(C)$；(b) $P(A\cap B)$，$P(A\cup C)$，$P(B\cap C)$. 这里 $A=\{$偶数$\}$，$B=\{2,3,4,5\}$，$C=\{1,2\}$.

7.69 设 A,B 为两个事件，且 $P(A)=0.7$，$P(B)=0.5$，$P(A\cap B)=0.4$. 求概率：(a) A 不发生；(b) A 或 B 发生；(c) A 发生但 B 不发生；(d) A、B 都不发生.

7.70 设 A,B 为两个事件. 且 $P(A)=0.6$，$P(B^c)=0.3$，$P(A\cup B)=0.8$. 求
(a) $P(A\cap B)$；　(b) $P(A\cap B^c)$；　(c) $P(A^c\cap B^c)$；　(d) $P(A^c\cup B^c)$.

条件概率，独立性

7.71 掷一个骰子，考虑事件 $A=\{2,4,6\}$，$B=\{1,2\}$，$C=\{1,2,3,4\}$. 求
(a) $P(A$ 与 $B)$，$P(A$ 或 $C)$.
(b) $P(A|B)$，$P(B|A)$.
(c) $P(A|C)$，$P(C|A)$.
(d) $P(B|C)$，$P(C|B)$.
(e) A 与 B 独立吗？A 与 C 呢？B 与 C 呢？

7.72 掷一对骰子. 若出现的数不相同. 求概率：
(a) 和为偶数.　(b) 和超过 9.

7.73 设 A,B 为两个事件，且 $P(A)=0.6$，$P(B)=0.3$，$P(A\cap B)=0.2$. 求
(a) $P(A\cup B)$；　(b) $P(A|B)$；　(c) $P(B|A)$.

7.74 设 A,B 为两个事件，且 $P(A)=\frac{1}{3}$，$P(B)=\frac{1}{4}$，$P(A\cup B)=\frac{1}{2}$.
(a) 求 $P(A|B)$ 与 $P(B|A)$.　(b) A 与 B 独立吗？

7.75 设 A,B 为两个事件，且 $P(A)=0.3$，$P(A\cup B)=0.5$，$P(B)=p$. 若(a) A 与 B 互不相交；(b) A 与 B 独立；(c) A 为 B 的子集，求 p.

7.76 设 A,B 为独立事件，且 $P(A)=0.3$，$P(B)=0.4$. 求
(a) $P(A\cap B)$ 与 $P(A\cup B)$；　(b) $P(A|B)$ 与 $P(B|A)$.

7.77 某国家俱乐部 60% 的成员打网球，40% 打高尔夫球，且 20% 既打网球又打高尔夫球. 现随机地选一名成员.
(a) 求他既不打网球又不打高尔夫球的概率.
(b) 若他打网球，求他打高尔夫球的概率.
(c) 若他打高尔夫球，求他打网球的概率.

7.78 盒 A 装有 6 个红弹子和 2 个蓝弹子，盒 B 装有 2 个红弹子和 4 个蓝弹子. 随机地从每个盒中各取出一个弹子.
(a) 求两个弹子都是红色的概率 p.
(b) 求一个红弹子，一个蓝弹子的概率 p.

7.79 A 击中目标的概率为 $\frac{1}{4}$，B 击中目标的概率为 $\frac{1}{3}$.
(a) 若每人开火两次，则至少击中一次目标的概率是多少？
(b) 若每人开火一次，且仅击中一次目标，则 A 击中目标的概率是多少？

7.80 掷 3 枚硬币. 考察事件：

$$A=\{\text{全为正面或全为反面}\},\quad B=\{\text{至少两个正面}\},\quad C=\{\text{至多两个正面}\}.$$

(A,B)，(A,C) 与 (B,C) 中哪一对是独立的？哪一对是相关的.

重复试验，二项分布

7.81 3 匹马 a,b,c 一起比赛，它们各自获胜的概率为 0.3，0.5 和 0.2. 现它们比赛 3 次.
(a) 求同一匹马赢得全部三场比赛的概率.
(b) 求 a,b,c 各赢得一场的概率.

7.82 某棒球选手的平均击球率为 0.300. 他击球 4 次. 求他(a) 恰两次击中;(b) 至少击中一次的概率.

7.83 Tom 在篮球的三分投篮时得分概率为 $p=0.4$. 他投篮 $n=5$ 次. 求他得分的概率:
(a) 恰投中两次; (b) 至少投中一次.

7.84 某队获胜(W)概率为 0.5,输(L)的概率为 0.3,平(T)的概率为 0.2. 该队比赛两次. (a) 确定样本空间 S 和每个基本事件的概率. (b) 求该队至少获胜一次的概率.

7.85 某种导弹击中目标概率为 $p=\frac{1}{3}$. (a) 若发射 3 枚导弹,求至少一次命中目标的概率. (b) 应发射多少枚导弹就可使得击中目标的概率至少为 90%.

随机变量

7.86 掷一对骰子,设 X 表示出现的两数中的最小数. 求 X 的分布与期望.

7.87 掷硬币 4 次,记 X 为正面朝上的最长串. 求 X 的分布及期望.

7.88 加重一枚硬币,使得 $p(H)=\frac{1}{3}$, $P(T)=\frac{2}{3}$. 投掷硬币直至出现一个正面或 5 个反面. 求投掷硬币次数的期望值.

7.89 A 队赢得任何比赛的概率为$\frac{1}{2}$. 假设 A 与 B 比赛,规定首先赢得连续两场或赢得 3 场比赛的队获胜. 求比赛中场数的期望值.

7.90 盒中装有 10 个晶体管,其中两个为次品. 从盒中取一个晶体管,并检测,直到选中一个正品. 求选取晶体管数的期望值.

7.91 500 张彩票设一个 100 美元奖, 3 个 50 美元奖和 5 个 25 美元奖.
(a) 求一张彩票的期望奖金.
(b) 若一张彩票花费一元. 求该局的期望值.

7.92 某选手掷 3 枚硬币. 若 3 个正面,则他赢 5 美元,若两个正面,则赢 3 美元,若仅一个正面则赢 1 美元. 另一方面,若 3 个反面,则他输 15 美元. 求比赛对该选手的值.

均值,方差与标准差

7.93 求下列每个分布的均值 μ,方差 σ^2 和标准差 σ.

(a)

x_i	2	3	8
p_i	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

(b)

x_i	−1	0	1	2	3
p_i	0.3	0.1	0.1	0.3	0.2

7.94 求下列两点分布的均值 μ,方差 σ^2 和标准差 σ,这里 $p+q=1$.

x_i	a	b
$f(x_i)$	p	q

7.95 从一个装有写着 1,1,2,2 和 3 的 5 张卡片的盒中抽取 2 张卡片. 设 X 表示抽出的两数之和,Y 表示抽出的两数的最大值,求下列随机变量的分布、均值、方差和标准差:
(a) X; (b) Y; (c) $Z=X+Y$; (d) $W=XY$.
($Z=X+Y$,$W=XY$的定义见问题 7.49.)

7.96 A 队参加比赛时获胜的概率为 $p=0.8$. 设 X 表示 A 在 $n=100$ 场比赛中将获胜的次数. 求 X 的均值 μ,方差 σ^2 和标准差 σ.

7.97 某未有准备的学生做 5 道判断题. 他猜每个答案. 若至少 4 个答案正确才通过. 求该生通过的概率.

7.98 设 X 为二项分布随机变量 $B(n,p)$. 且 $E(X)=2$, $\mathrm{Var}(X)=\frac{4}{3}$. 求 n 与 p.

补充题答案

7.53 (a) $A\cup B^c$； (b) $A\cap B^c$.

7.54 (a) $A\cap B\cap C^c$； (b) $(A\cup C)\cap B$； (c) $(A\cup B\cup B)^c=A^c\cap B^c\cap C^c$；
(d) $(A\cap B)\cup(A\cap C)\cup(B\cap C)$.

7.55 (a) $n(S)=24$； $S=\{H,T\}\times\{H,T\}\times\{1,2,\cdots,6\}$.
(b) $A=\{HH2,HH4,HH6\}$； $B=\{HH2,HT2,TH2,TT2\}$；
$C=\{HT1,HT3,HT5,TH1,TH3,TH5\}$.
(c) (i) HH2； (ii) HT2,TH2,TT2； (iii) $\varnothing$.

7.56 (a) $\frac{3}{6}$； (b) $\frac{15}{16}$； (c) $\frac{20}{36}$.

7.57 (a) $\frac{8}{18}$； (b) $\frac{3}{18}$； (c) $\frac{5}{18}$.

7.58 (a) $\frac{40}{50}$； (b) $\frac{10}{50}$； (c) $\frac{8}{150}$； (d) $\frac{42}{50}$.

7.59 (a) $\frac{1}{15}$； (b) $\frac{7}{15}$； (c) $\frac{8}{15}$； (d) $\frac{7}{15}$.

7.60 (a) $\frac{3}{10}$； (b) $\frac{3}{10}$； (c) $\frac{1}{15}$； (d) $\frac{8}{15}$.

7.61 $\frac{3}{5}$.

7.62 $\frac{1}{5}$.

7.63 (a) $\frac{3}{4}$； (b) $\frac{1}{4}$； (c) $\frac{1}{3}$； (d) $\frac{7}{12}$.

7.64 (a) $[4(3!)(3!)]/6!=\frac{1}{5}$； (b) $[2(3!)(3!)]/6!=\frac{1}{10}$.

7.65 (c)与(d).

7.66 $P(H)=\frac{3}{4}$； $P(T)=\frac{1}{4}$.

7.67 (a) $\frac{2}{5}$； (b) $\frac{1}{5}$； (c) $\frac{3}{5}$.

7.68 (a) 0.6,0.8,0.5； (b) 0.5,0.7,0.4.

7.69 (a) 0.3； (b) 0.8； (c) 0.2； (d) 0.2.

7.70 (a) 0.5； (b) 0.1； (c) 0.2； (d) 0.5.

7.71 (a) $\frac{1}{6},\frac{5}{6}$； (b) $\frac{1}{2},\frac{1}{3}$； (c) $\frac{1}{2},\frac{2}{3}$； (d) $\frac{1}{2}$,1； (e) 是,是,否.

7.72 (a) $\frac{12}{30}$； (b) $\frac{4}{30}$.

7.73 (a) 0.7； (b) $\frac{2}{3}$； (c) $\frac{[illegible]}{3}$.

7.74 (a) $\frac{1}{3},\frac{1}{4}$； (b) 是.

7.75 (a) 0.2； (b) $\frac{2}{7}$； (c) 0.5.

7.76 (a) 0.12,0.58； (b) $\frac{3}{10},\frac{4}{10}$.

7.77 (a) 20%； (b) $\frac{1}{3}$； (c) $\frac{1}{2}$.

7.78 (a) $\frac{1}{4}$； (b) $\frac{7}{12}$.

7.79 (a) $\frac{3}{4}$； (b) $\frac{1}{3}$.

7.80 仅(A,B).

7.81 (a) 0.16; (b) 0.18.

7.82 (a) $6(0.3)^2(0.7)^2=0.3456$; (b) $1-(0.7)^4=0.7599$.

7.83 (a) $10(0.4)^2(0.6)^3=0.2646$; (b) $1-(0.6)^5=0.92224$.

7.84 (b) P(WW, WT, TW) = 0.55.

7.85 (a) $1-\left(\frac{2}{3}\right)^3=\frac{19}{27}$; (b) 5次.

7.86

x_i	1	2	3	4	5	6
p_i	$\frac{11}{36}$	$\frac{9}{16}$	$\frac{7}{36}$	$\frac{5}{36}$	$\frac{3}{36}$	$\frac{1}{36}$

$E(X)=\frac{91}{36}\approx 2.5$.

7.87

x_i	0	1	2	3	4
p_i	$\frac{1}{16}$	$\frac{7}{16}$	$\frac{5}{16}$	$\frac{2}{16}$	$\frac{1}{16}$

$E(X)=\frac{27}{16}\approx 1.7$.

7.88 $\frac{211}{81}\approx 2.6$.

7.89 $\frac{23}{8}\approx 2.9$.

7.90 $\frac{11}{9}\approx 1.2$.

7.91 (a) 0.75; (b) −0.25.

7.92 0.25.

7.93 (a) $\mu=4, \sigma^2=5.5, \sigma=2.3$; (b) $\mu=1, \sigma^2=2.4, \sigma=1.5$.

7.94 $\mu=ap+bq$; $\sigma^2=pq(a-b)^2$; $\sigma=|a-b|\sqrt{pq}$.

7.95

(a)

x_i	2	3	4	5
$P(x_i)$	0.1	0.4	0.3	0.2

$E(X)=3.6$; $\mathrm{Var}(X)=0.84$; $\sigma_X=0.9$.

(b)

y_i	1	2	3
$P(y_i)$	0.1	0.5	0.4

$E(Y)=2.3$; $\mathrm{Var}(Y)=0.41$; $\sigma_Y=0.64$.

(c)

z_k	3	5	6	7	8
$P(z_k)$	0.1	0.4	0.1	0.2	0.2

$E(Z)=5.9$; $\mathrm{Var}(Z)=2.3$; $\sigma_Z=1.5$.

(d)

w_k	2	6	8	12	15
$P(w_k)$	0.1	0.4	0.1	0.2	0.2

$E(W)=8.8$; $\mathrm{Var}(W)=17.6$; $\sigma_W=4.2$.

7.96 $\mu=80$； $\sigma^2=16$； $\sigma=4$.

7.97 $\frac{6}{32}=\frac{3}{16}$.

7.98 $n=6$； $p=\frac{1}{3}$.

第八章　图　　论

8.1　引言,数据结构

数学与计算机科学的许多领域都出现了图、有向图、树以及二叉树.本章及下面两章将讨论这些专题.为了理解内存中如何存贮这些对象,理解有关它们的算法,我们应了解一些数据结构.假定读者理解线性及二维数组,因此下面我们只讨论链表与指针,堆栈与队列.

链表与指针

我们用一个例子来介绍链表与指针.假设一拍卖公司保存一个文件,该文件的每个记录包含顾客的姓名及公司店员,即文件包含以下数据:

顾客	Adams	Brown	Clark	Drew	Evans	Farmer	Geller	Hill	Infeld
店员	Smith	Ray	Ray	Jones	Smith	Jones	Ray	Smith	Ray

操作这些数据有两个基本运算:

运算 A:已知顾客姓名,求店员.

运算 B:已知店员姓名,求他的顾客的列表.

我们讨论在计算机中存贮数据,且易于对数据实施运算 A 和 B 的一些方法.

明显地,文件可以用一个九个姓名的两行(或列)的组存贮在计算机中.由于顾客按字母序排列,因此可方便地实施运算 A.然而,为实施运算 B,就必须查遍整个组.

利用二维组容易在存贮器存贮数据,二维组的行对应了顾客的字母序排列,列对应了店员的字母序排列.矩阵中有一个指明顾客的店员的 1,其余的为 0.如此表示的一个主要缺点就是大量的内存浪费,因为矩阵中有许多 0.例如,公司有 1000 名顾客和 20 个店员,存贮数据就需要 2000 个存贮位置,但其中只有 1000 个是有用的.

下面我们讨论用链表与指针在存贮器中存贮数据的方法.所谓*链表*是指数据元素的线性集,数据元素称为*点*,借助于指针域给出线性序.图 8-1 是 6 个点的链表的示意图,即每个点分为两个部分:第一部分包含了元素的信息(如,姓名,地址,…),第二部分称为*链域*或*后继指针域*,包含了表中后继点的地址.表中所画的从一点到另一点的箭头指出了指针域,图 8-1 还有一个指针变量,称为开始,它给出了表中第一个点的地址.此外,最后一个点的指针域有一个无效地址,称为*空指针*,它指明该表的结尾.

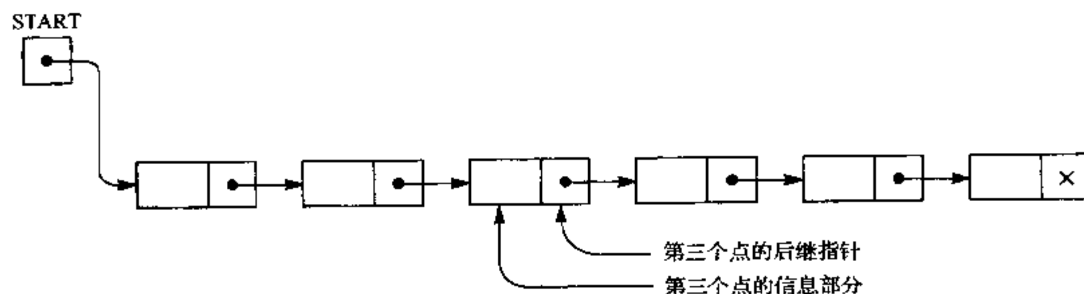
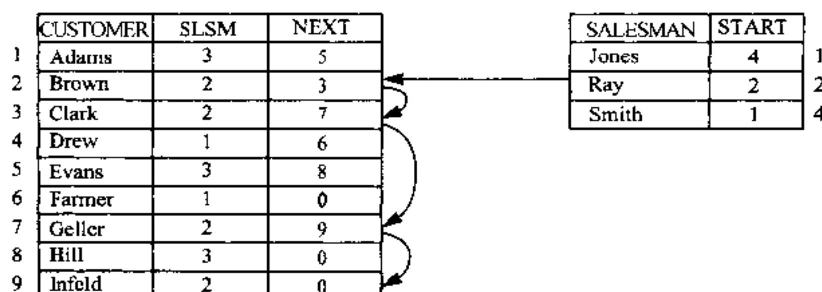


图 8-1　6 个点的链表

如图 8-2,利用链表存贮原始数据是一个主要方法.注意到对顾客与店员有可分的(字母序分类的)组.也有一个平行于 CUSTOMER(顾客)的指针组 SLSM,它给出顾客的店员的位置,因而运算 A 可以又快又方便地实施.进一步,如上面讨论,每个店员的顾客列表是一个链

表. 特别地,有一个平行于 SALESMAN(店员)的指针组 START,它指向店员的第一个顾客,有一个组 NEXT 指向店员的列表中后继顾客的位置(否则有一个 0,指明已是列表的结尾). 店员 Ray 的列表在图 8-2 中用箭头指出了这个过程.



	CUSTOMER	SLSM	NEXT
1	Adams	3	5
2	Brown	2	3
3	Clark	2	7
4	Drew	1	6
5	Evans	3	8
6	Farmer	1	0
7	Geller	2	9
8	Hill	3	0
9	Infeld	2	0

SALESMAN	START	
Jones	4	1
Ray	2	2
Smith	1	4

图 8-2

现在运算 B 能方便快速的实施. 也就是说,不必查遍全部的顾客就可得到给定店员的顾客列表. 下面给出这样的算法(用伪码编写).

算法 8.1 读取店员姓名,打印其顾客列表.

Step 1 读×××.

Step 2 求 K 使得 SALESMAN[K]=×××(用二叉查找).

Step 3 置 PTR:=START[K].(初始化指针 PTR)

Step 4 当 PTR≠NULL 时重复

(a)打印 CUSTOMER[PTR].

(b)置 PTR:=NEXT[PTR],(更新 PTR)

[结束循环]

Step5 退出

堆栈,队列,优先队列

除了组和链表外在图算法中还有其他数据结构,下面简单描述堆栈、队列和优先队列这些结构.

(a) 堆栈:堆栈也称为后进先出(LIFO)系统. 它是一个仅在表的称为"顶"的一端进行插入和删除的线性表. 这个结构在操作上类似于泉水系统中的碟栈的操作,如图 8-3(a). 注意到新的碟子只能在栈的顶部加入,也只能从栈的顶部拿走.



(a) 碟栈 (b) 等车队列

图 8-3

(b) 队列:队列也称为先进先出(FIFO)系统,它只能在表的称为前面的一端进行删除,而在表的另一个称为后面的一端进行插入. 这个结构的操作与在车站等车的人的队列非常一致. 如图 8-3(b),也就是说,队伍中的第一人第一个上车,新来的人排到队伍的后面.

(c) 优先队列:设 S 为新元素可以定期地插入,但总是删除当前最大的元素(具有最高优先权的元素)的一个元素集. 则 S 称为优先队列. 规则"妇女儿童优先"与"老人优先"就是优先队列的例子. 堆栈和普通队列也是特殊的优先队列. 特别地,堆栈中具有最高优先权的元素就

是插入的最后一个元素，而队列中的最高优先权元素就是元素第一个插入的.

8.2　图与多重图

一个图 G 由两个对象构成：

(i)集合 $V=V(G)$，其元素称为 G 的*顶点*或*点*.

(ii)集合 $E=E(G)$，其元素为 G 的不同顶点的无序偶，称为 G 的*边*.

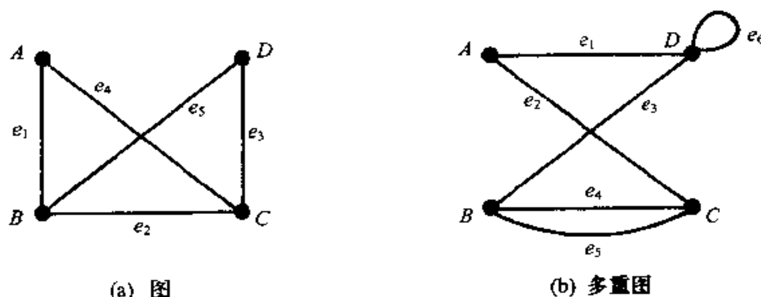
当要强调 G 的两个部分时，用 $G(V,E)$ 表示这样的图.

若存在一条边 $e=\{u,v\}$，则称顶点 u 和 v 为*相邻的*. 此时，u 与 v 称为 e 的*端点*，而称 e *连接* u 和 v，也称边 e 关联于它的端点 u 和 v.

图可以自然地在平面上表示出来. 特别地，V 的每个顶点 v 用一个点(或小圆圈)表示，每条边 $e=\{(v_1,v_2)\}$ 可用一条连接它的端点 v_1 和 v_2 的曲线来表示. 例如，图8-4(a)表示图 $G(V,E)$. 其中

(i) V 由顶点 A,B,C,D 构成.

(ii) E 由边 $e_1=\{A,B\},e_2=\{B,C\},e_3=\{C,D\},e_4=\{A,C\},e_5=\{B,D\}$ 构成.



(a) 图　　(b) 多重图

图 8-4

事实上，我们常用一个示意图来表示图，而不是明确地列出它的顶点与边.

多重图

考察图 8-4(b)中的示意图. 由于边 e_4 和 e_5 连接相同的端点，所以称它们为*重边*；而边 e_6 的两个端点是同一顶点，所以称 e_6 为*环*. 这样的图称为*多重图*. 图的正式定义中既不允许有重边也不允许有环. 因此，图可定义为没有重边和环的多重图.

注　一些教材中的图包括多重图，而用*简单图*表示没有重边和环的图.

顶点的度

图 G 中顶点 v 的*度* $\deg(v)$ 等于 G 中含 v 的边的条数，即关联于 v 的边数. 由于在计算 G 中顶点的度时，每条边被计数两次，于是有下面简单而重要的结果.

定理 8.1　G 中顶点的度之和等于 G 中边数的 2 倍.

例如，考虑图 8-4(a)中的图，有

$$\deg(A)=2,\ \deg(B)=3,\ \deg(C)=3,\ \deg(D)=2.$$

度的和为 10，正如所料的为边数的 2 倍. 根据顶点的度是偶数或是奇数，称这个点为*偶点*或*奇点*.

定理 8.1 对多重图也成立. 此时，一个环对环的端点的度算两次. 例如，在图 8-4(b)中，有 $\deg(D)=4$，因为边 e_6 被计两次，因此 D 为偶点.

度为 0 的顶点称为*孤立点*.

有限图，平凡图

若多重图的顶点数和边数都是有限的，则称它为*有限的*. 显然，具有有限个顶点的图其边

数也必为有限条,因而必为有限图.具有一个顶点而没有边即单点的图称为平凡图.除非特别指明,本书中的多重图是有限的.

8.3　子图,同构与同胚图

本节讨论图之间的一些重要关系.

子图

考虑图 $G=G(V,E)$,图 $H=H(V',E')$ 称为 G 的一个子图,如果 H 的顶点和边分别包含在 G 的顶点和边中,即 $V'\subseteq V$,且 $E'\subseteq E$.特别地:

(i) 若边集 E' 包含了 G 中端点在 H 中的所有边,则称图 $H(V',E')$ 为图 $G(V,E)$ 的由顶点 V' 导出的子图.

(ii) 若 v 为 G 的一个顶点,则 $G-v$ 是 G 的从 G 中删去顶点 v 以及 G 中含 v 的所有边所得到的子图.

(iii) 若 e 为 G 的一条边,则 $G-e$ 为从 G 中只删除边 e 所得到 G 的子图.

同构图

图 $G(V,E)$ 和 $G^*(V^*,E^*)$ 称为同构的,如果存在一个一一对应 $f:V\to V^*$ 使得 $\{u,v\}$ 为 G 的边当且仅当 $\{f(u),f(v)\}$ 为 G^* 的边.一般地我们对两个同构的图不加区分(即使它们的示意图也许看起来不同).图 8-5 给出 10 个画为字母的图.注意到 A 与 R 为同构图,F 与 T,K 与 X 以及 M,S,V 与 Z 也都是同构图.

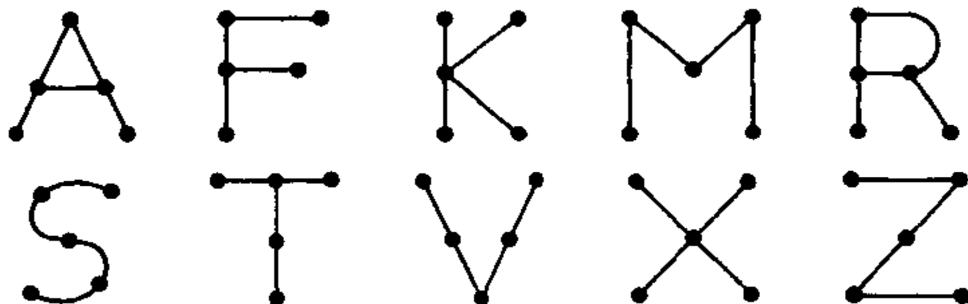


图 8-5

同胚图

给定图 G,可用另外的点剖分 G 的边得到一个新的图.两个图 G 和 G^* 称为同胚的,若它们能用这种方法从同一个图或从两个同构的图得到.图 8-6 中的图(a)和(b)不同构,但它们是同胚的,因为它们都可由图(c)添加适当的点得到.

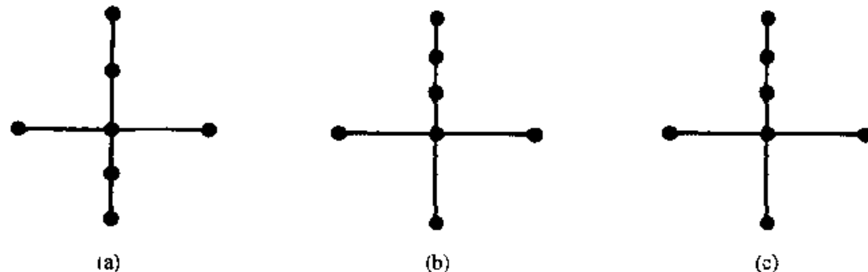


图 8-6

8.4 路,连通度

多重图 G 的路是由形如

$$v_0, e_1, v_1, e_2, v_2, \cdots, e_{n-1}, v_{n-1}, e_n, v_n$$

的点边交替序列构成,其中每条边 e_i 含有顶点 v_{i-1} 和 v_i(它们位于序列中 e_i 的两旁). 边数 n 称为这条路的长度. 在不引起混淆时,我们也用它的点序列($v_0, v_1, \cdots, v_n$)表示路. 若 $v_0 = v_n$,则称这条路为闭的. 否则称为从 v_0 到 v_n,或 v_0 与 v_n 之间,或连接 v_0 到 v_n 的路.

简单路是其顶点都不相同的路(边互不相同的路称为迹). 圈是除了 $v_0 = v_n$ 外,其余顶点互不相同的闭路. 长度为 k 的圈称为 k-圈. 图中的任意圈的长度至少为 3.

例 8.1 考虑图 8-7(a)中的图 G. 考虑以下序列:

$\alpha = (P_4, P_1, P_2, P_5, P_1, P_2, P_3, P_6)$, $\beta = (P_4, P_1, P_5, P_2, P_6)$,

$\gamma = (P_4, P_1, P_5, P_2, P_3, P_5, P_6)$, $\delta = (P_4, P_1, P_5, P_3, P_6)$.

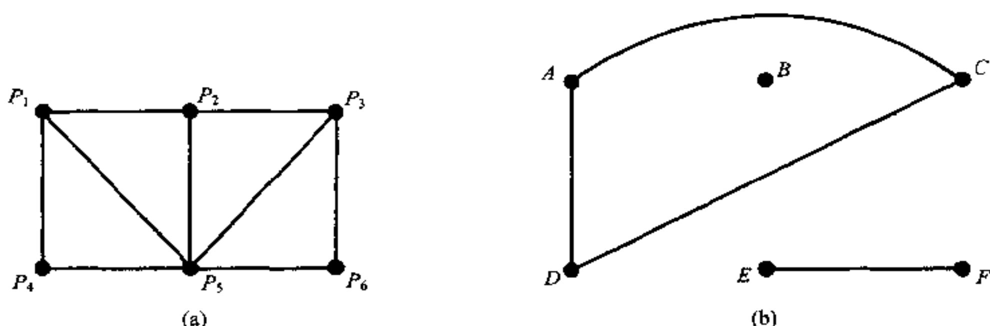


图 8-7

序列 α 为从 P_4 到 P_6 的路,但不是迹,因为边 $\{P_1, P_2\}$ 被用了两次. 序列 β 不是路,因为没有边 $\{P_2, P_6\}$. 序列 γ 是迹,因为没有边被用了两次. 但不是简单路,因为顶点 P_5 用了两次. 序列 δ 是从 P_4 到 P_6 的简单路,但不是从 P_4 到 P_6 的最短路(关于长度而言). 从 P_4 到 P_6 的最短路是简单路(P_4, P_5, P_6),其长为 2.

去除不必要的边,不难看出任一条从顶点 u 到顶点 v 的路可用从 u 到 v 的简单路取代. 这一事实可正式地叙述如下:

定理 8.2 存在从顶点 u 到顶点 v 的路当且仅当存在从 u 到 v 的简单路.

连通度,连通分支

图 G 称为连通的,如果它的任两点之间都存在一条路. 图 8-7(a)中的图是连通的,但图 8-7(b)中的图不是连通的,因为,例如,顶点 D 和 E 之间没有路.

设 G 为一个图,G 的一个连通子图 H 称为 G 的连通分支,如果 H 不含在 G 的任何更大的连通子图中. 直观上易见任何图 G 可以划分为一些连通分支. 例如,图 8-7(b)中的图有三个连通分支,分别是由顶点集 $\{A, C, D\}$,$\{E, F\}$ 和 $\{B\}$ 导出的子图.

图 8-7(b)中的顶点 B 称为孤立点,因为 B 不属于任何一条边,换句话说,$\deg(B) = 0$. 因此,B 本身构成该图的一个连通分支.

注 正式地说,假设任意点都连到自身,则关系"u 连到 v"是图 G 的顶点集上的一个等价关系,并且这个关系的等价类构成了 G 的连通分支.

距离与直径

考虑连通图 G. G 中顶点 u 与 v 之间的距离 $d(u, v)$ 就是 u 与 v 之间最短路的长度. G 的直径 $\mathrm{diam}(G)$ 为 G 中任两点之间距离的最大值. 例如,在图 8-8(a)中,$d(A, F) = 2$,$\mathrm{diam}(G) = 3$. 而在图 8-8(b)中,$d(A, F) = 3$,$\mathrm{diam}(G) = 4$.

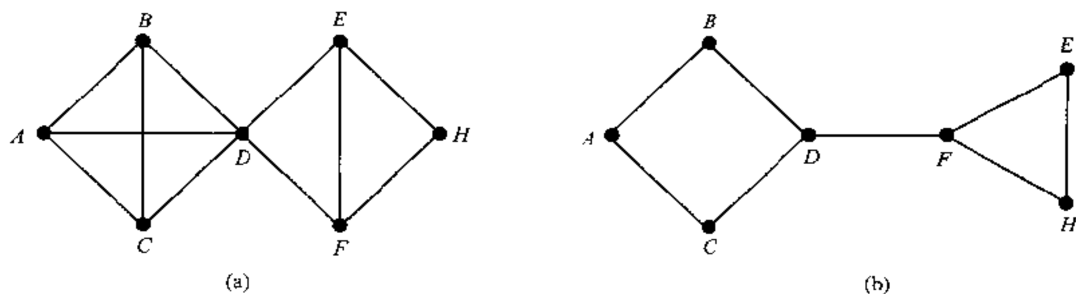


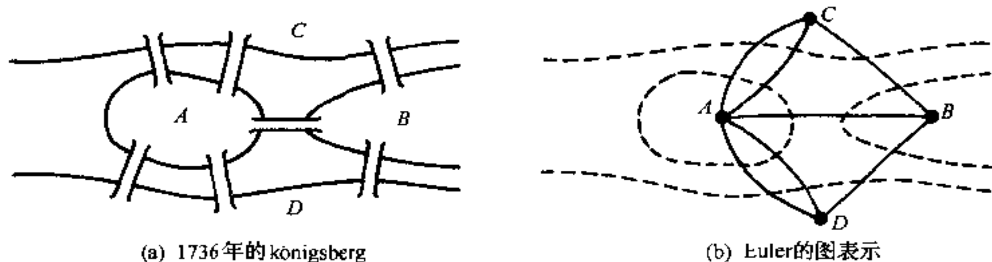
图 8-8

割点与桥

设 G 为连通图. G 的顶点 v 称为割点，如果 $G-v$ 不连通.（回忆 $G-v$ 是从 G 中删去 v 以及含有 v 的所有边所得到的图.）G 的边 e 称为桥，如果 $G-e$ 不连通.（回忆 $G-e$ 是从 G 中删去边 e 所得到的图）. 在图 8-8(a)中，顶点 D 是割点，没有桥. 在图 8-8(b)中，边 $e=\{D,F\}$ 是桥.（其端点 D 和 F 必然为割点.）

8.5　Königsberg 桥，可旅行多重图

18 世纪 Königsberg 的东 Prussian 镇有两个岛与七座桥，如图 8-9(a). 问题：人们能否从该镇的任一处开始环城散步，经过全部七座桥，但不经过任何桥两次，而回到任一处? Königsberg 的人们将这个问题写信告诉了著名的瑞士数学家 L. Euler. Euler 在 1736 年证明了这样的散步是不可能的. 他用点代表岛及河的两边，用曲线代表桥，得到图 8-9(b).

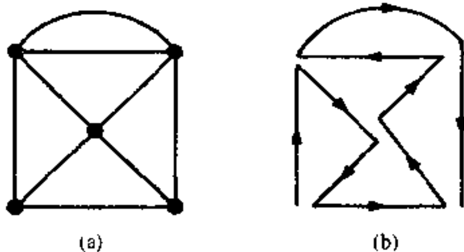


(a) 1736年的 königsberg　　　(b) Euler的图表示

图 8-9

注意到图 8-9(b)是多重图. 多重图称为可旅行的，如果它"能不间断地用曲线画出而没有边重复". 即如果存在一条包含所有顶点，且每条边恰用一次的路. 这样的路必定是迹(因为没有边用两次，称为可旅行迹). 显然，可旅行的多重图必须是有限的和连通的，图 8-10(b)给出了图 8-10(a)中多重图的可旅行迹.（为说明该迹的方向，该图略去实际通过的接触点.）不难看出 königsberg 城的散步是可能的当且仅当图 8-9(b)中的多重图是可旅行的.

现在我们解释 Euler 是如何证明图 8-9(b)中的多重图是不可旅行的，因而 königsberg 的这种散步也是不可能的. 首先回忆一个顶点根据它的度数是偶数或奇数，该点就为偶点或奇点. 假设多重图是可旅行的，且可旅行迹不是以 P 开始与结束. 我们断言 P 为偶点. 因为一旦可旅行迹由一条边进入 P，则必存在一条前面未用的边，该迹以这条边离开 P. 于是该迹中与 P 关联的边必成对出现，因此 P 为偶点. 因此，若顶点 Q 为奇点，则可旅行迹必以 Q 开始或结束，于是，多于两个奇点的多重图不可能是可旅行的. 注意到对应于 königsberg 桥问题的多重图有 4 个奇点，因而人们不能环 königsberg



(a)　　　(b)

图 8-10

城散步，使得每座桥恰好经过一次.

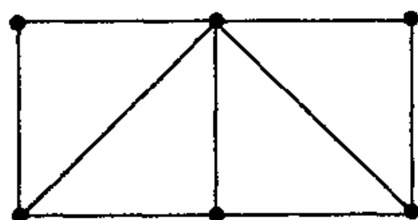
Euler实际上证明了上述问题的反问题，它含在下面的定理与推论中.（定理在问题8.9中证明.）图G称为是Euler图，如果存在一条闭可旅行迹（称为Euler迹）.

定理 8.3(Euler) 有限连通图是Euler图当且仅当其每个顶点的度数为偶数.

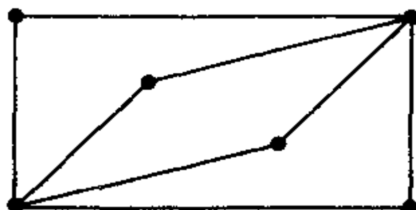
推论 8.4 两个奇点的有限连通图是可旅行的.可旅行迹可以从任一奇点开始，另一奇点结束.

Hamilton 图

上面Euler图的讨论强调了旅行边，这里关注访问点.图G的*Hamilton回路*，以19世纪以色列数学家W. Hamilton(1805~1865)的名字命名，是G的一条经过每个顶点恰一次的闭路.（这样的闭路必为圈.）若G有一个Hamilton回路，则G称为Hamilton图.注意Euler回路通过每条边恰一次，但允许顶点重复，而Hamilton回路则通过每个顶点恰好一次，此时边必不相同*.图8-11给出了是Hamilton图但不是Euler图的例子，也给出了是Euler图但不是Hamilton图的例子.



(a) Hamilton图而非Euler图



(b) Euler图而非Hamilton图

图 8-11

尽管显然只有连通图才可能为Hamilton图，但没有简单的法则使我们能判别一个图是否为Hamilton图，而对Euler图则有简单的法则. G. A. Dirac给出了下面的充分条件.

定理 8.5 设G为n个顶点的连通图.若$n\geqslant 3$，且对G的每个顶点v有$\deg(v)\geqslant n$，则G为Hamilton图.

8.6 标号图与赋权图

图G称为*标号图*，如果它的边与/或顶点被指定一种或另一种数据.特别地，G称为*赋权图*，如果G的每条边e被指派一个称为e的*权*或*长度*的非负数.图8-12给出了一个赋权图，每条边的权明确地给出.在这样的赋权图G中，路的*权*（或*长度*）定义为该路上边的权的和.图论中的一个重要问题就是求*最短路*，即两个给定顶点之间的最小权（长度）的路.图8-12中P与Q之间的最短路的长度为14.$(P,A_1,A_2,A_5,A_3,A_6,Q)$就是这样一条路.读者可尝试求另一条最短路.

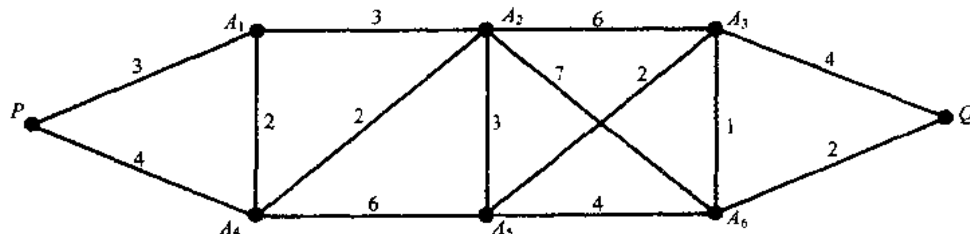


图 8-12

* 译者注：原书"边可以重复"有误.

8.7 完全图,正则图与二部图

图有各种各样的类型,本节讨论其中三个:完全图,正则图与二部图.

完全图

如果 G 的每个顶点都与 G 中每个其他顶点有边相连接,则图 G 称为是完全图. 于是,完全图必是连通的. n 个顶点的完全图记为 K_n. 图 8-13 给出了 K_1 到 K_6.

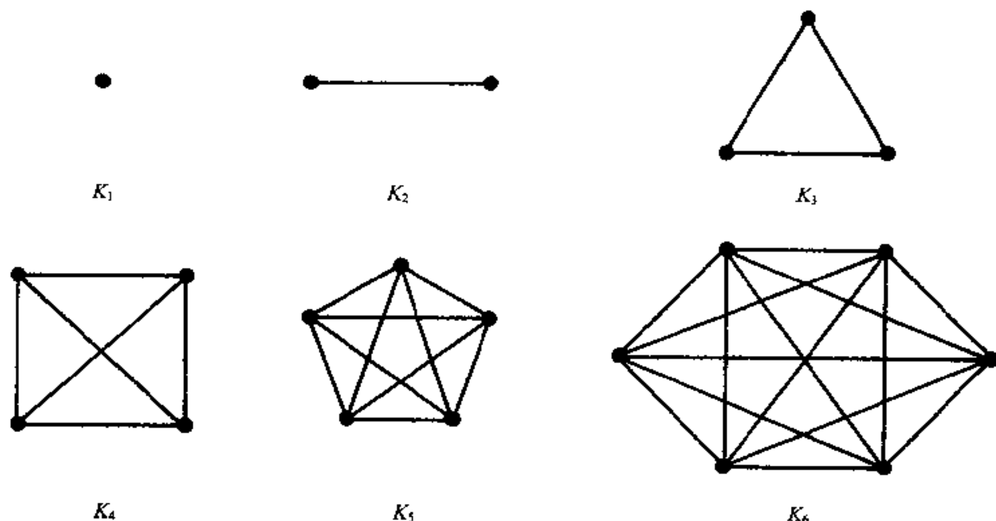


图 8-13

正则图

如果图 G 的每个顶点的度为 k,则称图 G 为 k 度正则的,或 k-正则的. 换句话说,如果每个顶点有相同的度,则图是正则的.

容易描述连通的 0 度,1 度,2 度正则图. 连通 0-正则图就是一个顶点没有边的平凡图. 连通 1-正则图就是两个顶点以及连接它们的一条边的图. n 个顶点的连通 2-正则图是一个的 n-圈. 见图 8-14.

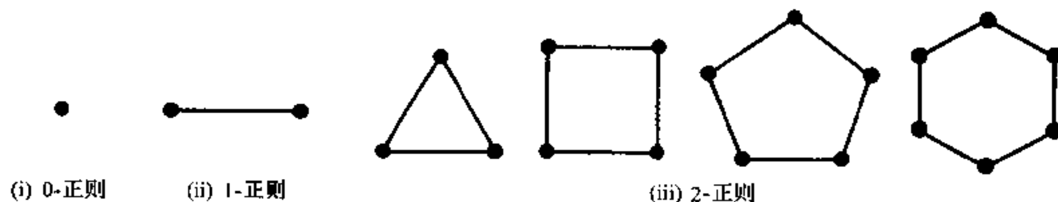


图 8-14 正则图

3-正则图必有偶数个顶点,因为顶点的度之和为偶数(定理 8.1). 图 8-15 给出了 2 个 6 个顶点的连通 3-正则图. 一般地,正则图可能很复杂. 例如,存在 19 个 10 个顶点的3-正则图. 注意到 n 个顶点的完全图 K_n 是 $n-1$ 度正则的.

二部图

图 G 称为二部图,如果它的顶点集 V 可以划分为两个子集 M 和 N,使得 G 的每条边连接 M 的一个点到 N 的一个点. 完全二部图是指 M 的每个顶点连到 N 的每个顶点. 这种图记为 $K_{m,n}$,其中 m 为 M 中的顶点数,n 为 N 中的顶点数,且为标准化,约定$m\leqslant n$. 图 8-16 给出了

图 $K_{2,3}$，$K_{3,3}$和 $K_{2,4}$，显然，图 $K_{m,n}$有 mn 条边.

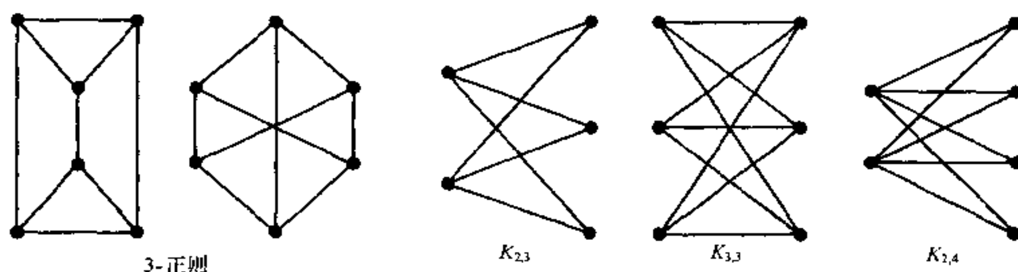


图 8-15　　　　图 8-16

8.8 树图

图 T 称为树，如果 T 是连通的且没有圈. 图 8-17 给出树的例子. 森林 G 是一个没有圈的图. 因此，森林 G 的连通分支都是树.（没有圈的图称为无圈图.）没有边的单个顶点的树称为退化树.

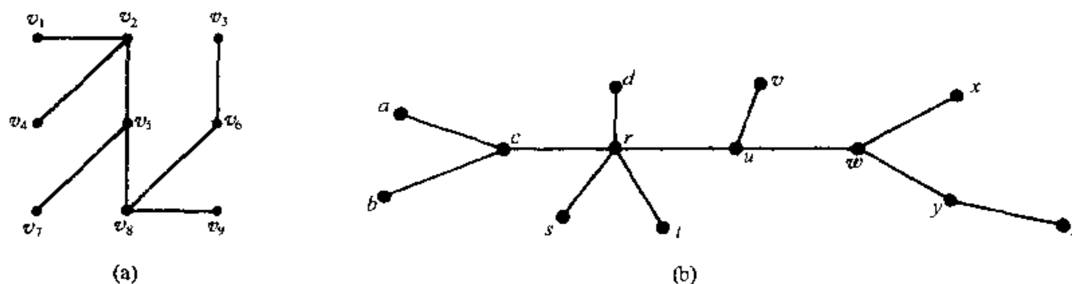


图 8-17

考虑树 T. 显然，T 的两点之间只有一条简单路. 否则这两条路将构成一个圈. 也有

(a)　假设 T 中没有边$\{u,v\}$，且对 T 添加边 $e=\{u,v\}$. 则 T 的从 u 到 v 的简单路与 e 构成一个圈，因此 T 不再是树.

(b)　另一方面，假设 $e=\{u,v\}$为 T 的一条边，并从 T 中删除 e. 则 T 不再连通（因为不能有从 u 到 v 的路），因此，T 不再是树.

下面的定理（在问题 8.16 中证明）对有限图适用.

定理 8.6　设 G 为 $n>1$ 个顶点的图，则下列结论等价：

(i)G 是树.

(ii)G 为无圈图，且有 $n-1$ 条边.

(iii)G 连通，且有 $n-1$ 条边.

这个定理也告诉我们 n 个顶点的有限树 T 必有 $n-1$ 条边. 例如，图 8-17(a)中的树有 9 个顶点和 8 条边，图 8-17(b)中的树有 13 个顶点和 12 条边.

支撑树

连通图 G 的子图 T 称为 G 的支撑树，如果 T 是树，且包含了 G 的所有顶点. 图 8-18 给出了连通图 G 及 G 的支撑树 T_1，T_2 和 T_3.

最小支撑树

设 G 为连通的赋权图，即 G 的每条边被指定了一个称为边的权的非负数，则 G 的每个支撑树被指定了一个 T 中每条边的权之和的总权. G 的最小支撑树就是总权尽可能小的支撑树.

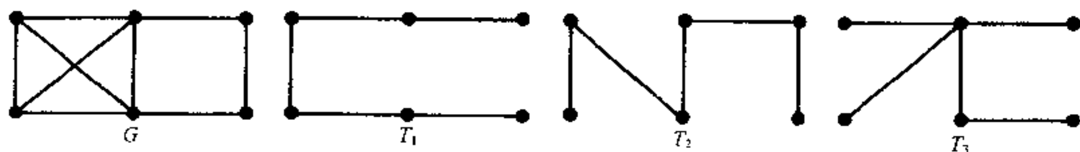


图 8-18

算法 8.8A 和 8.8B 使我们能求 n 个顶点连通赋权图的最小支撑树.(无论哪一种情形,T 必有 $n-1$ 条边.)

> **算法 8.8A** 输入 n 个顶点的连通赋权图 G.
>
> **Step 1** 按权递减的序排列 G 的边.
>
> **Step 2** 相继地依序删去未使 G 不连通的边,直至剩下 $n-1$ 条边.
>
> **Step 3** 退出.

> **算法 8.8B(Kruskal)** 输入 n 个顶点的连通赋权图 G.
>
> **Step 1** 按权递增的序排列 G 的边.
>
> **Step 2** 仅用 G 的顶点,相继依序添加不产生圈的边,直至添加了 $n-1$ 条边.
>
> **Step 3** 退出.

最小生成树的权是惟一的,但最小生成树本身并不是惟一的.当两条或多条边有相同的权时,就可能产生不同的最小支撑树.此时,算法 8.8A 或 8.8B 中第一步边的排列不惟一,因而有可能产生不同的最小支撑树,我们举例说明这一点.

例 8.2 求图 8-19(a)中赋权图 Q 的最小支撑树.注意 Q 有 6 个顶点,故最小支撑树将有 5 条边.

(a) 应用算法 8.8A.

首先按递减权的序排列边,然后相继删除不导致 Q 不连通的边,直至剩下 5 条边.于是有下面的数据:

边	BC	AF	AC	BE	CE	BF	AE	DF	BD
权	8	7	7	7	6	5	4	4	3
删除?	是	是	是	否	否	是			

这样得到的 Q 的最小支撑树含有边 BE,CE,AE,DF,BD.该支撑树的权为 24,如图 8-19(b).

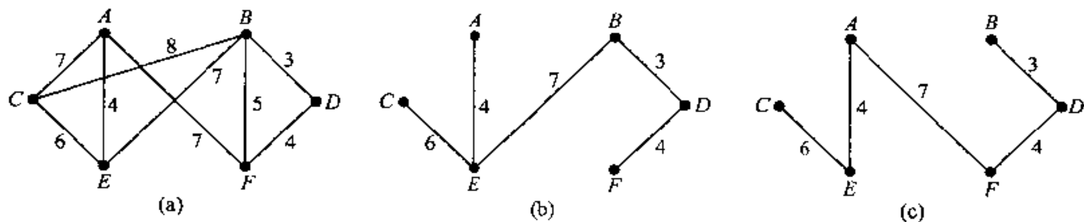


图 8-19

(b) 应用算法 8.8B.

首先按权递增的序排列边,然后添加不致产生圈的边,直至有了 5 条边.于是有下列数据:

边	BD	AE	DF	BF	CE	AC	AF	BE	BC
权	3	4	4	5	6	7	7	7	8
增加?	是	是	是	否	是	否	是		

因此这样得到的 Q 的最小支撑树含有边 BD,AE,DF,CE,AF. 如图 8－19(c). 注意这个支撑树与算法 8. 8A 得到支撑树不同.

注　当图 G 像图 8－19(a)相当小时，上面的算法容易执行. 假如 G 有成百的顶点和边，这些边由一列点对给出. 那么甚至确定 G 是否连通也不那么容易，它也许需要某种深度优先查找(DFS)或广度优先查找(BFS)的图算法. 后面几节以及下一章将讨论存贮中表示图 G 的方法以及各种图算法.

8.9　平面图

能够画在平面上使得它的边不相交叉的图或多重图称为平面图. 尽管 4 个顶点的完全图 K_4 通常画有相交叉的边，如图 8－20(a)，但它也能如图 8－20(b)画成没有交叉边的图. 因此 K_4 是平面图，树图是重要的平面图类. 本节给读者介绍这些重要的图.

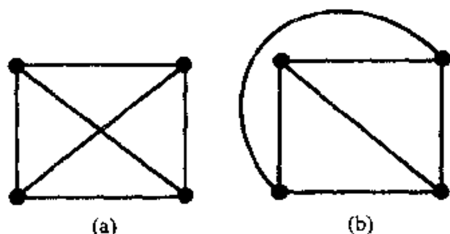


图 8－20

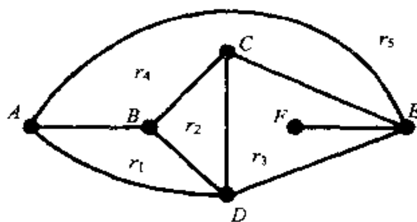


图 8－21

地图，区域

有限平面多重图的特定平面表示称为地图. 称地图是连通的，如果其基础多重图是连通的. 任一给定地图将平面分成各种区域. 例如，图 8－21 中 6 个顶点，9 条边的地图将平面分为 5 个区域. 注意到其中 4 个区域是有界的，但第 5 个区域在图形的外面，是无界的. 因此，不失一般性，在计算区域数时，我们可以假设地图含在某个大的矩形而不是整个平面中.

注意地图的每个区域的边缘由边构成，有时这些边形成一个圈，有时不是. 例如，在图 8－21中，除 r_3 外的所有区域的边缘都是圈. 然而，若我们从顶点 C 开始，沿 r_3 逆时针移动，则得到闭路(C,D,E,F,E,C)，其中边$\{E,F\}$出现了两次. 区域 r 的度 $\deg(r)$是指围绕 r 的圈或闭路的长度. 注意到每条边或者围绕了两个区域，或者含在一个区域内. 因此，在沿着区域的边缘的任何路中都出现两次. 由此，类似于对顶点的定理 8. 1，对区域有下面的定理.

定理 8.7　地图区域的度的和等于边数的两倍.

图 8－21 的区域的度为

$$\deg(r_1)=3,\ \deg(r_2)=3,\ \deg(r_3)=5,\ \deg(r_4)=4,\ \deg(r_5)=3,$$

度和为 18，正好等于边数的两倍.

为方便计，用点或小圆圈表示地图的顶点. 否则我们就假设平面上两直线或曲线的相交处是顶点.

Euler 公式

Euler 给出了联系任何连通地图的顶点数 V，边数 E 以及区域数 R 的一个公式. 也就是，

定理 8. 8(Euler)　$V-E+R=2$.

(定理 8. 8 的证明在问题 8. 20 中.)

注意到，在图 8－21 中，$V=6$，$E=9$，$R=5$，且正如所料，由 Euler 公式得

$$V-E+R=6-9+5=2.$$

要强调的是，为使 Euler 公式成立，地图的基础图必须连通.

设 G 为 3 个或更多顶点的连通平面多重图，因而 G 既不是 K_1 也不是 K_2. 令 M 为 G 的平

面表示.不难看出:(1) 仅当 M 的区域的边缘是一个环,则该区域可以是 1-度区域,(2) 仅当 M 的区域的边缘为两条重边时,该区域的度才为 2. 于是,若 G 是图,而不是多重图,则 M 的每个区域的度必定至少为 3. 利用这个结论以及 Euler 公式可证下面的有关平面图的结果.

定理 8.9　设 G 为连通平面图,有 p 个顶点和 q 条边,$p\geqslant 3$. 则 $q\leqslant 3p-6$.

注意该定理对 K_1 不成立,此时 $p=1,q=0$. 且对 K_2 也不成立,此时 $p=2,q=1$.

证明　设 r 为 G 的平面表示的区域数,由 Euler 公式,

$$p-q+r=2.$$

由定理 8.7,区域的度和等于 $2q$. 但每个区域的度至少为 3,因此

$$2q\geqslant 3r.$$

于是,$r\leqslant 2q/3$. 在 Euler 公式中替换 r,得

$$2=p-q+r\leqslant p-q+\frac{2q}{3},$$

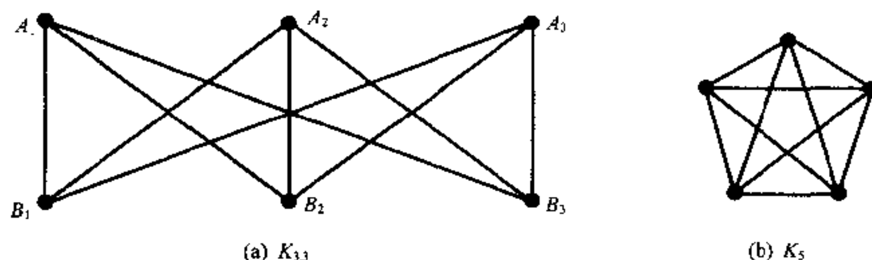
即

$$2\leqslant q-\frac{q}{3}$$

两边同乘以 3 便给出结果.

非平面图,Kuratowski 定理

先给两个非平面图的例子. 先考虑应用图,即三座房屋 A_1,A_2,A_3 要连接到水、电、气 B_1,B_2,B_3 的接口,如图 8-22(a). 注意这是图 $K_{3,3}$,它有 $p=6$ 个顶点,$q=9$ 条边. 假设该图是平面的. 由 Euler 公式,其平面表示有 $r=5$ 个区域. 注意到没有三个点相互邻接. 因此每个区域的度是 4 或更大,由此,区域的度和至少为 20. 再由定理 5.9,该图至少有 10 条边,但这与该图只有 $q=9$ 条边矛盾. 因此应用图 $K_{3,3}$ 是非平面图.



(a) $K_{3,3}$　　(b) K_5

图 8-22

接下来考虑图 8-22(b)中的星图. 这是 $p=5$ 个顶点,$q=10$ 条边的完全图 K_5. 若该图是平面的,则由定理 8.9,

$$10=q\leqslant 3p-6=15-6=9$$

矛盾. 因此 K_5 是非平面的.

多少年来,数学家尝试刻画平面图与非平面图. 这个问题在 1930 年被波兰数学家 K. Kuratowski最终解决. 由于证明超出本书的范围,我们仅将这个结果叙述如下:

定理 8.10(Kuratowski)　图是非平面的当且仅当它含有同胚于 $K_{3,3}$或 K_5 的子图.

8.10　图着色

考虑图 G,G 的顶点着色,简称为着色,是给 G 的每个顶点指定一个颜色,使得相邻的顶点有不同的颜色. 若存在用 n 种颜色的 G 的着色,则称 G 为 n-可着色的. (由于词"着色"常用作名词,为避免将它用作动词,因此在给 G 的顶点指派颜色时,用染色而不用着色.) 染色 G 所需的最少颜色数称为 G 的色数,并记为 $\chi(G)$.

Welch 和 Powell 给出了图 G 着色的算法，但要注意这个算法并不总是给出 G 的最小着色.

算法 8.10(Welch-Powell) 输入一个图 G.

Step 1 根据度递减的次序排列 G 的顶点.

Step 2 给第一个顶点染第一种颜色 C_1，然后，依次序给与前面已染 C_1 的点不相邻的点染 C_1.

Step 3 用第二种颜色对未染色点的子序列重复 Step 2.

Step 4 用第三种颜色，第四种颜色，……重复 Step 3，直至所有点都已染色.

Step 5 退出.

例 8.3 (a)考虑图 8－23 中的图 G. 用 Welch-Powell 算法 8.10 得到 G 的着色. 根据度递减的次序排列顶点给出下面的序列：

$$A_5, A_3, A_7, A_1, A_2, A_4, A_6, A_8$$

给 A_5 和 A_1 涂第一种颜色，给 A_3，A_4 和 A_8 涂第二种颜色，对 A_7，A_2，A_6 涂第三种颜色，则所有顶点都已被染色，因此 G 是 3－可着色的.

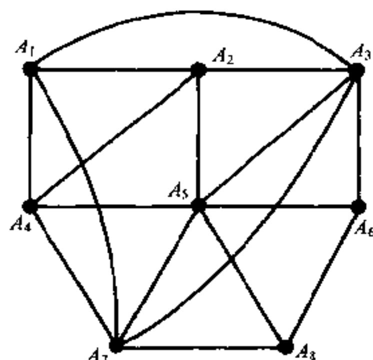


图 8－23

注意 G 不是 2－可着色的，因为顶点 A_1，A_2 和 A_3 是相互连接的. 因此必须具有不同的颜色，由此，$\chi(G)=3$.

(b) 考虑 n 个顶点的完全图 K_n. 因为每个顶点都连接到其他每个点，因此在任何着色中，K_n 需要 n 种颜色，于是 $\chi(K_n)=n$.

实际上，没有简单的方法确定任意图 G 是否 n－可着色的. 不过，下面的定理(证明在问题 8.22 中)给出了 2－可着色图的简单刻画.

定理 8.11 对图 G，下面结论等价：

(i) G 为 2－可着色的.

(ii) G 为二部图.

(iii) G 的每个圈有偶长度.

任意图的着色所需的颜色数是没有限制的. 因为，比如说，完全图 K_n 需要 n 种颜色. 然而，如果我们只讨论平面图，那么无论顶点数是多少，4 种颜色就行的. 特别地，在问题 8.24 中我们证明了：

定理 8.12 任何平面图是 5－可着色的.

实际上，由于每个已知的平面图都是 4－可着色的，所以自 1850 年以来，数学家就猜想：平面图是 4－可着色的. 在 1976 年，Apple 和 Haken 终于证明了这个猜想是对的. 即

四色定理(Apple 和 Haken) 任意平面图是 4－可着色的.

我们在下一节讨论这个定理.

对偶地图与四色定理

考虑地图 M，比方说图 8－24(a)中的地图 M. 即 M 为平面多重图的平面表示. M 的两个区域若有公共的边，则称为相邻. 于是图 8－24(a)中的区域 r_2 和 r_5 是相邻的，但区域 r_3 和 r_5 不相邻. M 的着色是指对 M 的区域的颜色指派，使得相邻的区域有不同的颜色. 若存在 M 的用 n 个颜色的着色，则称 M 是 n－可着色的. 于是图 8－24(a)中的地图 M 是 3－可着色的，因为各区域可如下涂色：r_1 红色，r_2 白色，r_3 红色，r_4 白色，r_5 红色，r_6 蓝色. 注意到这个着色地图

的讨论与前面着色图的讨论的相似性. 用下面定义的对偶地图的概念,事实上,可以证明,地图的着色等价于平面图的顶点着色.

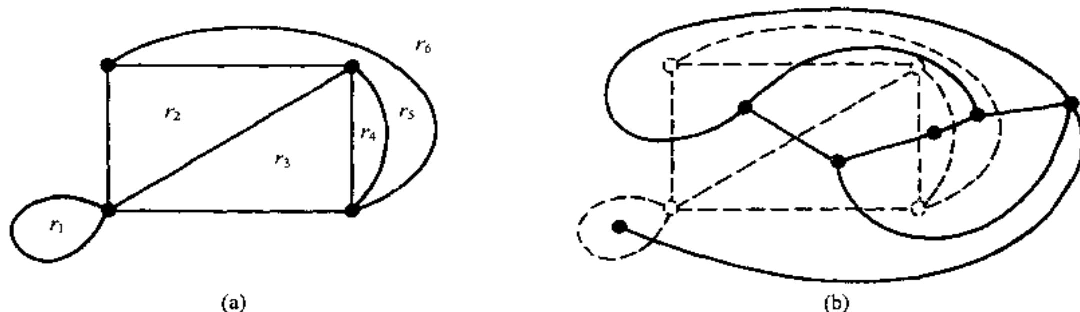


图 8 - 24

考虑地图 M,在 M 的每个区域内取一个点. 若两区域有公共边,则用一条通过这条公共边的曲线连接相应的两个点. 这些曲线可以画的互不相交,于是得到一个新的地图 M^*,称为 M 的对偶. 使得 M^* 的每个点恰对应 M 的一个区域. 图 8 - 24(b)给出了图8 - 24(a)中地图的对偶. 可以证明 M^* 的每个区域恰含 M 的一个点,且 M^* 的每条边恰与 M 的一条边相交,反之亦然. 因此 M 也为地图 M^* 的对偶.

注意到地图 M 的任意区域着色对应着对偶地图 M^* 的顶点着色. 因此,M 是 n -可着色的当且仅当对偶地图 M^* 的平面图是顶点 n -可着色的. 上面的定理可如下叙述:

四色定理(Appel 和 Haken) 要使任意地图 M 的相邻区域着不同颜色,则至多需要四种颜色.

上面这个定理的证明本质上使用了计算机. 特别地,Appel 和 Haken 首先证明了若四色定理不成立,则在近 2000 多种平面图中存在一个反例. 然后他们借助计算机证明了这些图中没有这样的反例. 若不使用计算机,则每种图的检验都似乎超出了人类的能力. 因此,与数学的多数证明不同,该证明与技术相关,即依赖于高速计算机的发展.

8.11 在计算机存贮器中的表示图

有两个标准方法将图 G 存贮在计算机中. 一种称为 G 的*序列表示*,即借助于图的邻接矩阵 A. 另一种称为 G 的*链表示*或*邻接结构*,采用了邻点的链表. 当图 G 稠密时常用矩阵表示,而当图 G 稀疏时常用链表. (设图 G 有 m 个顶点 n 条边. 如果 $m=O(n^2)$,则图 G 是稠密的;如果 $m=O(n)$ 或 $O(n\log n)$,则图 G 是稀疏的.)

无论用什么方法存贮图 G,图 G 都用它的正式定义输入到计算机,即用顶点集和点对(边)集输入到计算机.

邻接矩阵

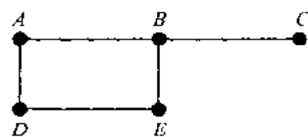
设 G 为 m 个顶点的图,并设顶点已排序为 $v_1,v_2,\cdots,v_m$. 则图 G 的*邻接矩阵* $A=[a_{ij}]$ 就是如下定义的 $m\times m$ 矩阵:

$$a_{ij}=\begin{cases}1,\text{若 } v_i \text{ 连接到 } v_j,\\0,\text{否则.}\end{cases}$$

图 8 - 25(b)给出了图 8 - 25(a)中图 G 的邻接矩阵,其中顶点排序为 A,B,C,D,E. 注意 G 的每条边 $\{v_i,v_j\}$ 用 $a_{ij}=1$ 和 $a_{ji}=1$ 表示两次. 因此,邻接矩阵是对称的.

图 G 的邻接矩阵 A 依赖于 G 的顶点的次序,即不同的顶点序给出不同的邻接矩阵. 然而,任两个这样的邻接矩阵是紧密联系的,因为一个邻接矩阵可以从另一个邻接矩阵通过简单地交换行、列得到. 另一方面,邻接矩阵并不依赖于阶数,它将边(顶点对)输入到计算机的次序.

上述表示有各种变形. 若 G 为多重图,常用 a_{ij} 表示边 $\{v_i,v_j\}$ 的数目. 此外,若 G 为赋权



(a)

$$
\begin{array}{c|ccccc}
 & A & B & C & D & E \\
\hline
A & 0 & 1 & 0 & 1 & 0 \\
B & 1 & 0 & 1 & 0 & 1 \\
C & 0 & 1 & 0 & 0 & 0 \\
D & 1 & 0 & 0 & 0 & 1 \\
E & 0 & 1 & 0 & 1 & 0
\end{array}
$$

(b)

图 8 - 25

图，可用 a_{ij} 表示边 $\{v_i, v_j\}$ 的权.

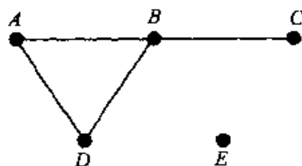
图 G 的链表示

设 G 为 m 个顶点的图，用图 G 的邻接矩阵 A 存贮 G 有诸多不便. 首先在 G 中插入或删除顶点是困难的. 因为 A 的大小可能需要改变，且顶点也可能需要重新排序，从而矩阵 A 也会有众多繁杂变化. 进一步，假如 G 的边数是 $O(m)$ 或 $O(m\log m)$，即假如 G 是稀疏的，那么矩阵 A 中含有许多 0. 因而大量的存贮空间浪费了. 因此，当 G 稀疏时，G 常用某种链表示，也称为邻接结构来存贮，借助于一个例子描述.

考虑图 8 - 26(a) 中的图 G. 注意 G 可用图 8 - 26(b) 中的表等价地定义，这个表给出了 G 的每个顶点以及它的邻接表. 即它的邻接点（邻点）的表. 用符号 $\varnothing$ 表示空邻接，这个表也可以紧凑地表示为

$$G=[A:B,D;\quad B:A,C,D;\quad C:B;\quad D:A,B;\quad E:\varnothing].$$

这里冒号":"分隔顶点与它的邻点，而分号";"分隔不同的列表.



(a)

顶点	邻接表
A	B,D
B	A,C,D
C	B
D	A,B
E	∅

(b)

图 8 - 26

注 注意图 G 的每条边在邻接结构中表示两次，即任一边，如 $\{A, B\}$ 在 A 的邻接表中用 B 表示，在 B 的邻接表中又表示为 A. 图 8 - 26(a) 中的图 G 有 4 条边. 因而在邻接表中必须有 8 个顶点. 另一方面，邻接表中的每个顶点对应了图 G 中的惟一边.

图 G 的邻接表示，即用它的邻接表存贮 G，通常含有两个文件（或记录集），一个称为点文件，另一个称为边文件. 如下定义：

(a) **点文件** 点文件包含图 G 的顶点列表. 它用一个组或链表存贮，点文件的每个记录有如下形式

VERTEX	NEXT-V	PTR	

其中 VERTEX 为顶点的名字. 当顶点以链表存贮时，NEXT-V 指向点文件的顶点列表的后继点. 而 PTR 指向边文件中出现的点的邻接列表的第一个元素. 阴影区域表示对应于该点的记录可能还有其他信息.

(b) **边文件** 边文件包含图 G 的边. 特别地，边文件包含 G 的所有邻接表，而每个表以链表存贮. 边文件的每个记录对应于邻接表的一个顶点，因此，间接地对应于 G 的一条边. 记录通常有如下形式

EDGE	ADJ	NEXT	

其中(1) EDGE 为边的名字(若有的话).

(2) ADJ 指向点文件中顶点的位置.

(3) NEXT 指向邻接表中后继顶点的位置.

注意,每条边在边文件中表示两次,但文件的每个记录对应了惟一的边. 阴影区域表明对应于该边的记录中可能有的其他信息.

图 8-27 给出了图 8-26(a)中图 G 是如何存贮的. G 的顶点以链表存贮,它采用了指向第一个顶点的变量 START.(因此,若采用线性组代替顶点列表,则 NEXT-V 将不再需要.)注意由于这些边没有名字,所以字段 EDGE 不是必需的. 图 8-27 也用箭头表示了顶点 B 的邻接表$[D,C,A]$.

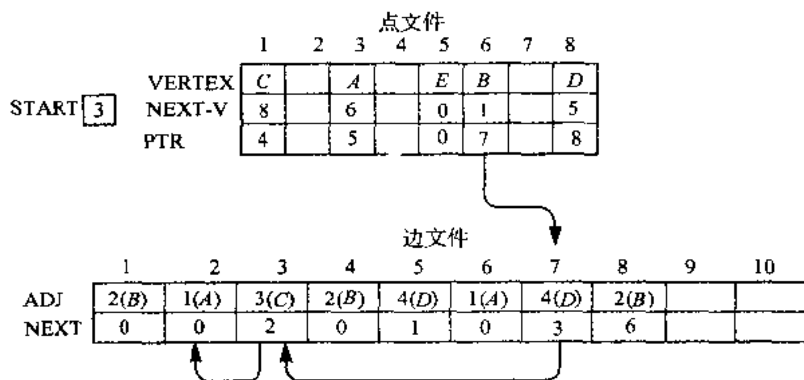
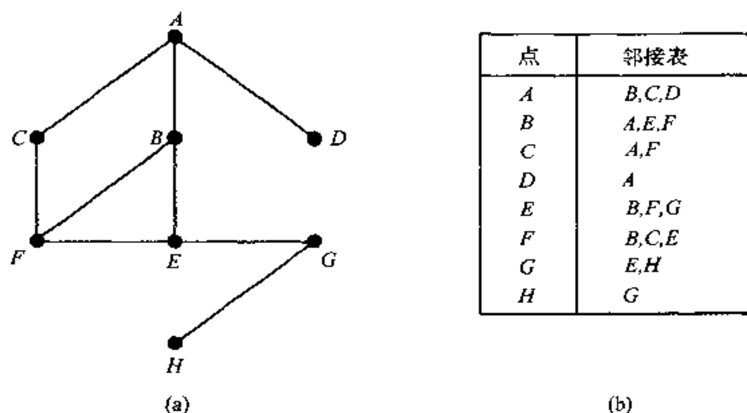


图 8-27

8.12 图算法

本节讨论两个重要的图算法,它系统地检查图 G 的顶点和边. 一个称为*深度优先查找*(DFS),另一个称为*广度优先查找*(BFS). 下一章再讨论与有向图有关的其他图算法. 任何特别的图算法可能依赖于 G 的存贮方式. 这里假设 G 用其邻接结构存贮,用图 8-28 中的图 G 作为测试图,它给出了图 G 的邻接结构.



点	邻接表
A	B,C,D
B	A,E,F
C	A,F
D	A
E	B,F,G
F	B,C,E
G	E,H
H	G

图 8-28

在执行算法时,G 的每个顶点(点)N 有下面三种状态之一,称为 N 的状态(STATUS):

STATUS=1:(准备状态)　顶点 N 的初始状态.

STATUS=2:(等候状态)　顶点 N 在(等候)表中,等待进行.

STATUS=3:(检查状态)　顶点 N 已检查.

深度优先查找的等候表是一个(修改的)堆栈,而广度优先查找的等候表是一个队列.

深度优先查找

下面给出从顶点 A 开始的深度优先查找的一般概念. 首先检查开始点 A，然后沿着由 A 开始的路 P 检查每个顶点 N. 即检查 A 的邻点，再检查 A 的邻点的邻点，等等. 在到达“死点”后，即到达一个没有未检查的邻点的点后，我们追踪 P 直到可沿着另一条路 P' 继续，如此等等. 用一个拥有未来可能路的初始点的堆栈来实现反向追踪. 现需要一个字段 STATUS 来表示每个点的当前状态，以便使得没有点检查超过一次，算法如下：

算法 8.12A（深度优先查找） 该算法从一个开始点 A 开始执行图 G 的深度优先查找.

Step 1 初始化所有点到准备状态（STATUS=1）.

Step 2 从开始点 A 放到堆栈上，并将 A 的状态改为等候状态（STATUS=2）.

Step 3 重复 Step 4 和 Step 5，直到堆栈空.

Step 4 取堆栈的“顶”点 N，检查 N，并置 STATUS(N)=3 检查状态.

Step 5 检查 N 的每个邻点 J.

(a) 若 STATUS(J)=1（准备状态），把 J 放到堆栈上，重置 STATUS(J)=2（等候状态）.

(b) 若 STATUS(J)=2（等候状态），从堆栈中删去前一个 J，把当前 J 放到堆栈上.

(c) 若 STATUS(J)=3（检查状态），略过顶点 J.

[结束 Step 3 循环]

Step 6 退出.

上面算法只检查了连到开始顶点 A 的那些点，即只检查了含 A 的连通分支. 假设要对图 G 的所有顶点检查，那么算法必须修改，使得它再开始于另一个顶点（称为 B），该点仍处于准备状态（堆栈=1），该点 B 可走遍顶点列表得到.

注 上面算法中的结构堆栈技术上不是堆栈，因为，在 Step 5(b)中，允许删除顶点 J，然后插到这个堆栈的前面.（尽管是同一个顶点 J，但在邻域结构中它通常表示不同的边.）若在 Step 5(b)不移动 J，则得到 DFS 的另一形式.

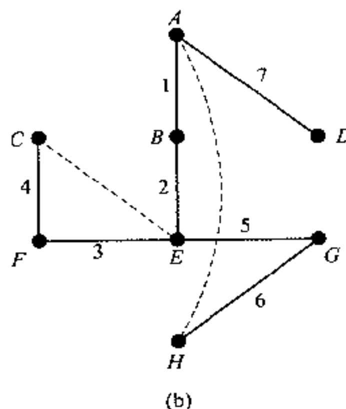
例 8.4 对图 8-28 中的图应用 DFS 算法 8.12A. 顶点按下列次序进行.

$$A, B, E, F, C, G, H, D.$$

特别地，图 8-29(a)给出了 STACK 的等待列表的序列及将进行的顶点. 用斜杠“/”表示从这个等候列表中删除一个点. 每个顶点，不包括 A，源于一个邻接表因而对应于该图的一条边，这些边构成了 G 的一棵支撑树，如图 8-29(b)，数字给出加到树上边的顺序，虚线指出反向追踪.

顶点	堆栈
	A
A	B,C,D
B	E,F,C,D
E	F,G,~~F~~, C,D
F	C,G,~~C~~,D
C	G,D
G	H,D
H	D
D	

(a)



(b)

图 8-29

广度优先查找

下面给出广度优先查找的一般概念，它从一个起始点 A 开始. 首先检查起始点 A，然后检查 A 的所有邻点，再检查 A 的邻点的邻点，如此等等. 自然地，需要保留顶点的邻点的轨迹，还要保证没有顶点检查两次. 这由队列和字段 STATUS 完成. 队列包含了等待检查的点. 而 STATUS 告诉我们顶点的当前状态. 算法如下

算法 8.12B(广度优先查找)　该算法执行图 G 的广度优先算法，它从一个起始点 A 开始.

Step 1　初始化所有顶点到准备状态(STATUS=1).

Step 2　将起始点 A 放进队列，并将 A 的状态改变为等候状态(STATUS=2).

Step 3　重复 Step 4 和 Step 5，直到队列空.

Step 4　移去队列的前面点 N，检查 N，并置 STATUS(N)=3，检查状态.

Step 5　检查 N 的每个邻点 J.

(a) 若STATUS(J)=1(准备状态)，将 J 加到队列的后面. 重置 STATUS(J)=2(等候状态).

(b) 若 STATUS(J)=2(等候状态)或 STATUS(J)=3(检查状态)，跳过顶点 J.

[结束 Step 3 循环]

Step 6　退出.

上面的算法还是仅进行那些连接到起点 A 的点，即含 A 的连通分支. 假设要对图 G 的所有顶点检查，算法就必须修改，使得它再开始于另一个顶点(称为 B)，该点仍处于准备状态(STATUS=1)，这个顶点可通过走遍顶点列表得到.

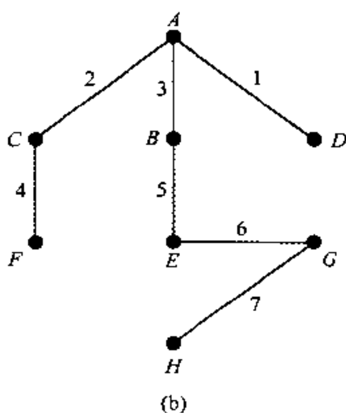
例 8.5　对图 8-28 中的图应用 BFS 算法 8.12B. 顶点按以下顺序检查：

$$A,\ D,\ C,\ B,\ F,\ E,\ G,\ H.$$

特别地，图 8-30(a)给出队列的等待表的序列以及正在检查的顶点. 再一次，除 A 外的每个顶点仍来自于邻接列表，因而对应于图 G 的一条边，这些边构成了 G 的一棵支撑树，如图 8-30(b)，同样数字指出添加到树上边的顺序. 注意这个支撑树与图 8-29(b)中的由深度优先查找得到的支撑树不同.

顶点	队列
	A
A	B,C,D
D	B,C
C	F,B,
B	E,F
F	E
E	G
G	H
H	

(a)



(b)

图 8-30

问题与解答

图术语

8.1 考虑图 8-31.(a) 正式描述画出的图 G,即求 G 的顶点集 $V(G)$ 和边集 $E(G)$.(b) 求每个顶点的度,并对此图验证定理 8.1.

解 (a) 有 5 个顶点,因此,$V(G)=\{A,B,C,D,E\}$.有 7 个点对 $\{x,y\}$ 使得 x 连到 y,故

$$E(G)=[\{A,B\},\{A,C\},\{A,D\},\{B,C\},\{B,E\},\{C,D\},\{C,E\}].$$

(b) 顶点的度数等于该顶点属于的边数.例如,由于 A 属于三条边 $\{A,B\},\{A,C\},\{A,D\}$,故 $\deg(A)=3$.类似地,

$$\deg(B)=3,\ \deg(C)=4,\ \deg(D)=2,\ \deg(E)=2,$$

顶点的度之和为

$$3+3+4+2+2=14,$$

等于边数的 2 倍.

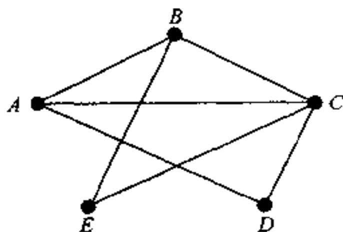


图 8-31

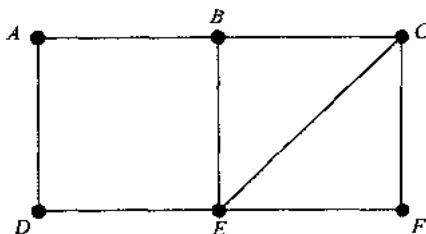


图 8-32

8.2 考虑图 8-32 中的图 G.求(a) 从 A 到 F 的所有简单路;(b) 从 A 到 F 的所有迹;(c) 从 A 到 F 的距离 $d(A,F)$;(d) G 的直径 $\operatorname{diam}(G)$;(e) 包含 A 的所有圈;(f) G 中的所有圈.

解 (a) 从 A 到 F 的简单路是一条没有顶点,因而也没有边重复的路.有 7 条这样的路,4 条以边 $\{A,B\}$ 开头,3 条以边 $\{A,D\}$ 开头:

$$(A,B,C,F),\ (A,B,C,E,F),\ (A,B,E,F),\ (A,B,E,C,F);$$
$$(A,D,E,F),\ (A,D,E,B,C,F),\ (A,D,E,C,F).$$

(b) 从 A 到 F 的迹是没有边重复的路,有 9 条这样的迹:(a)中的 7 条简单路以及 (A,D,E,B,C,E,F) 和 (A,D,E,C,B,E,F).

(c) 有一条从 A 到 F 长为 3 的路,如 (A,B,C,F),而没有更短的从 A 到 F 的路,因此 $d(A,F)=3$.

(d) 任两点之间的距离不超过 3,且从 A 到 F 的距离为 3.因此,$\operatorname{diam}(G)=3$.

(e) 圈是顶点(除起点与终点)不重的闭路,有 3 个圈含顶点 A.

$$(A,B,E,D),\ (A,B,C,E,D,A),\ (A,B,C,F,E,D,A).$$

(f) G 中有 6 个圈,(e)中的 3 个以及 (B,C,E,B),(C,F,E,C),(B,C,F,E,B).

8.3 考虑图 8-33 的多重图 G.(a) 哪些是连通的?若图不连通,求它的连通分支.(b) 哪些是无圈的?(c) 哪些是无环的?(d) 哪些是图?

解 (a) 只有(1)和(3)是连通的,(2)不连通,它的连通分支是 $\{A,D,E\}$ 和 $\{B,C\}$.(4) 不连通,它的连通分支是 $\{A,B,E\}$ 和 $\{C,D\}$.

(b) 仅(1)和(4)是无圈的,(2)有圈 (A,D,E,A),(3)有圈 (A,B,E,A).

(c) 只有(4)有环,该环为 $\{B,B\}$.

(d) 只有(1)和(2)是图.多重图(3)有重边 $\{A,E\}$ 和 $\{A,E\}$,且(4)有重边 $\{C,D\}$ 和 $\{C,D\}$,还有环 $\{B,B\}$.

8.4 设 G 为图 8-34(a)中的图.求:(a) 从 A 到 C 的所有简单路;(b) 所有的圈;(c) G 的由 $V'=\{B,C,X,Y\}$ 生成的子图 H;(d) $G-Y$;(e) 所有割点;(f) 所有桥.

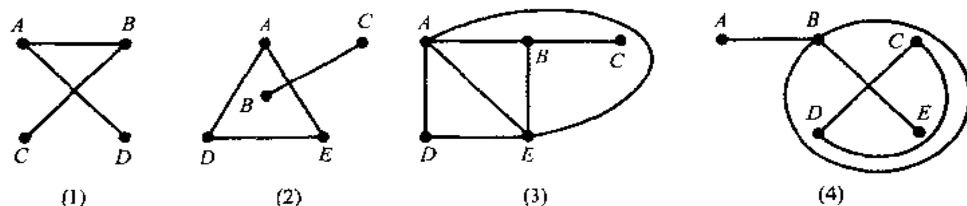


图 8 - 33

解 (a) 从 A 到 C 的简单路有两条:(A,X,Y,C) 和 (A,X,B,Y,C).

(b) 只有一个圈 (B,X,Y,B).

(c) 如图 8 - 34(b),H 由顶点集 V' 及端点在 V' 中的所有边的集合 E' 构成,即

$$E'=[\{B,X\},\{X,Y\},\{B,Y\},\{C,Y\}].$$

(d) 从 G 中删去 Y 以及含 Y 的所有边就得到图 8 - 34(c)中的图 $G-Y$.(注 Y 为割点,因为 $G-Y$ 不连通.)

(e) 顶点 A,X 和 Y 是割点.

(f) 若 $G-e$ 不连通,则边 e 称为桥.于是,存在 3 个桥:$\{A,Z\}$,$\{A,X\}$ 和 $\{C,Y\}$.

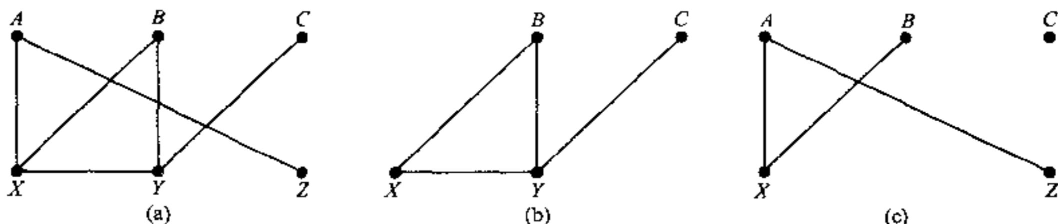


图 8 - 31

8.5 考虑图 8 - 32 的图 G.求删去一个顶点所得的子图,G 有割点吗?

解 从 G 中删去一点,也必须删去含有该点的所有边.删去一点得到 6 个这样的图,见图 8 - 35,所有这 6 个图都是连通的,因而没有割点.

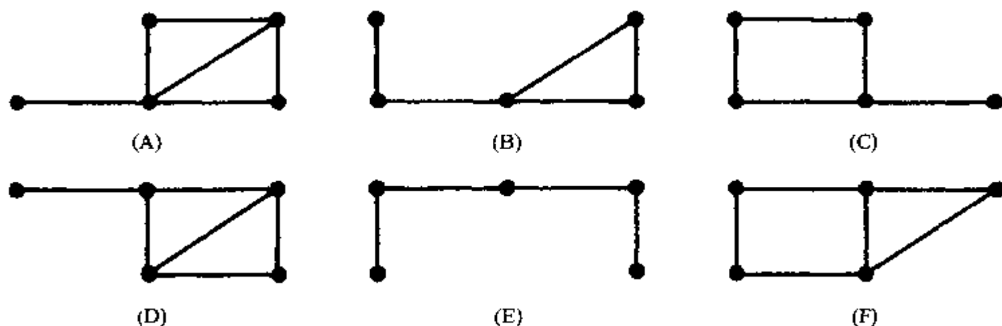


图 8 - 35

8.6 证明问题 8.5 中得到的 6 个图是不同的,即这些图中没有两个图是同构的.并证明(B)和(C)同胚.

证 除了(B)和(C),任何图的 5 个顶点的度都不能与其他图的度相配,因此,除了可能(B)和(C)外,没有图同构.

然而,若删去(B)和(C)中的 3 度点.则得到不同的子图,因此(B)和(C)也不同构,因而所有 6 个图都不相同.但(B)和(C)是同胚的,因为它们可分别从图 8 - 36 的同构图添加适当的点得到.

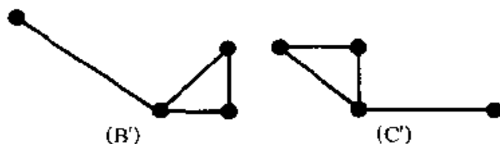


图 8 - 36

可旅行图,Euler 回路与 Hamilton 回路

8.7 考虑图 8 - 37 中的每个图 G. 哪些是可旅行的,即有 Euler 路? 哪些是 Euler 图,即有 Euler 回路? 若不是,说明理由.

解 ☞ 若 G 仅有 0 或 2 个顶点的度为奇数,则 G 可旅行的(有 Euler 路),若 G 的所有顶点的度都是偶数,则 G 是欧拉图(有 Euler 回路).

(a) 可旅行的,因为有两个奇点,可旅行路必以一个奇点开始,以另一奇点结束.

(b) 可旅行的,因为所有点为偶点,因而有 Euler 回路.

(c) 因为 6 个顶点为奇点,所以 G 不是可旅行的.

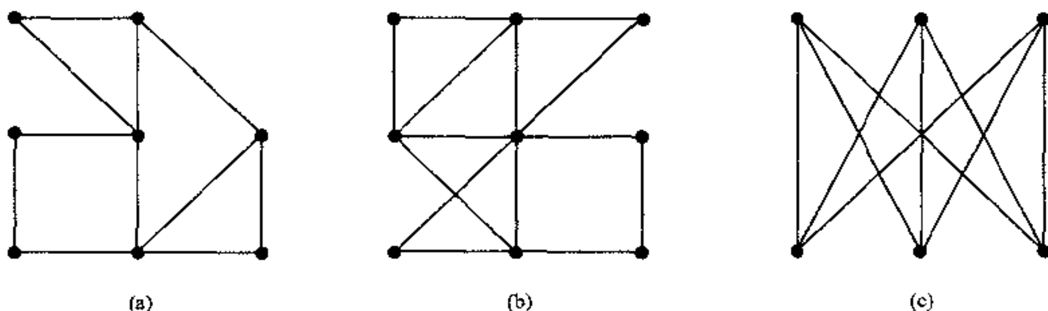


图 8 - 37

8.8 图 8 - 37 中的哪些图有 Hamilton 回路? 若没有,为什么?

解 ☞ 图(a)和(c)有 Hamilton 回路(读者应能方便地找到其中一条). 然而图(b)没有 Hamilton 回路. 因为若 α 是一条 Hamilton 回路,则 α 必将中间点连接到其左下的点,然后沿着底行移到下面的右点,再垂直到中间的右点,但在走遍剩下的点之前就被迫回到中心点.

8.9 证明定理 8.3(Euler):有限连通图 G 是 Euler 的当且仅当每个点有偶度.

证 ☞ 设 G 为 Euler 的,且 T 为 Euler 闭迹. 对 G 的每个顶点 v,迹 T 进入和离开 v 相同的次数,且边不重复,因此 v 有偶度.

反过来,假设 G 的每个点有偶度,现构造 Euler 迹. 从任一条边 e_1 开始迹 T_1,一条一条地添加边扩展 T_1. 若在任何时候,T_1 都不是闭的,比方说,T_1 开始于 u,但在 $v \neq u$ 结束. 因此,T_1 中关联于 v 的边仅有奇数条出现,因而可用另一条关联于 v 的边扩展 T_1. 这样继续扩展 T_1,直到 T_1 返回到其出发点 u,即 T_1 为闭的. 若 T_1 包含了 G 的所有边,则 T_1 为 Euler 迹.

假设 T_1 不含 G 的所有边,考虑从 G 中删去 T_1 的所有边得到的图 H. H 也许不连通,但 H 的每个点的度数为偶数,因为 T_1 含关联于任一点的偶数条边. 由于 G 是连通的,故存在 H 的边 e',它有一个端点 u' 在 T_1 中. 在 H 中从 u' 开始,并用边 e' 构造迹 T_2. 因为 H 的所有顶点是偶度数,所以可在 H 中继续扩展 T_2,直到 T_2 返回到 u',如图 8 - 38. 显然,将 T_1 和 T_2 放在一起构成图 G 中更大的闭迹. 继续这个过程直到用遍 G 中的所有边. 最后便得到了 Euler 迹,因而 G 是 Euler 的.

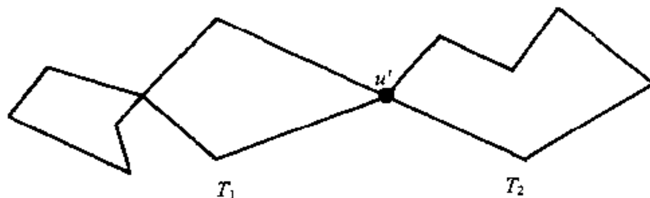


图 8 - 38

特殊图

8.10 画图 $K_{2,5}$.

解 ☞　$K_{2,5}$ 含有 7 个点，分成 2 点 u_1 和 u_2 的集合 M 和 5 点 $v_1,v_2,\cdots,v_5$ 的集合 N，也含有所有可能的从顶点 u_i 到 v_j 的边. 于是有 10 条边. 如图 8－39.

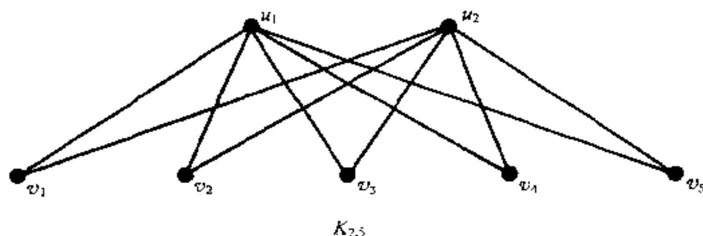


图 8－39

8.11　哪些连通图既是正则的又是二部的？

解 ☞　二部图 $K_{m,m}$ 是 m－度正则的，因为每个点连到 m 个其他的点. 因此它的度为 m. 从中删去 m 条不相交边所得的 $K_{m,m}$ 的子图也是正则的，例如图 8－40 给出的 $K_{4,4}$ 的子图是3－正则的. 可以继续删去 m 条不相交的边，每次得到少一度的正则图. 这些图可能是不连通的，但无论怎样，它们的连通分支具有所需性质.

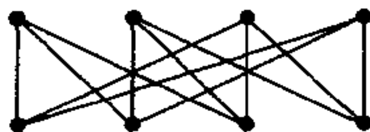


图 8－40

树，支撑树

8.12　画出恰 6 个顶点的所有树.

解 ☞　有 6 个这样的树，如图 8－41. 第一棵树直径为 5，接着的两棵树直径为 4，再接下来的两棵树直径为 3，最后一棵树直径为 2. 任何其他 6 个点的树必同构于这些树之一.

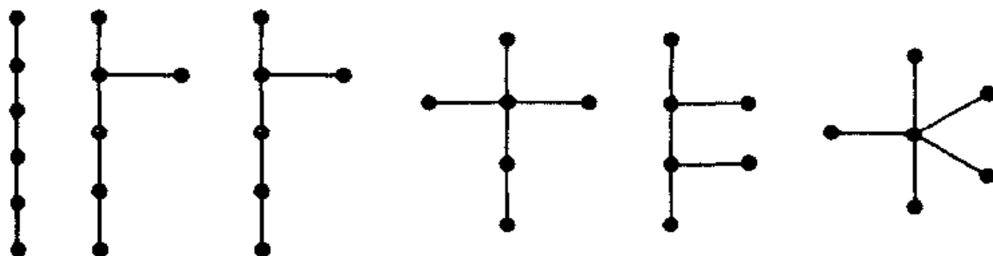


图 8－41

8.13　求图 8－42(a)中图 G 的所有支撑树.

解 ☞　如图 8－42(b)，有 8 个这样的支撑树，每个支撑树必有 $4-1=3$ 条边，因为 G 有 4 个顶点. 由此每个支撑树可从 G 的 5 条边中删去 2 条边得到. 这有 10 种方法，除去其中两个给出不连通图. 因此，上面 8 个支撑树为 G 的所有支撑树.

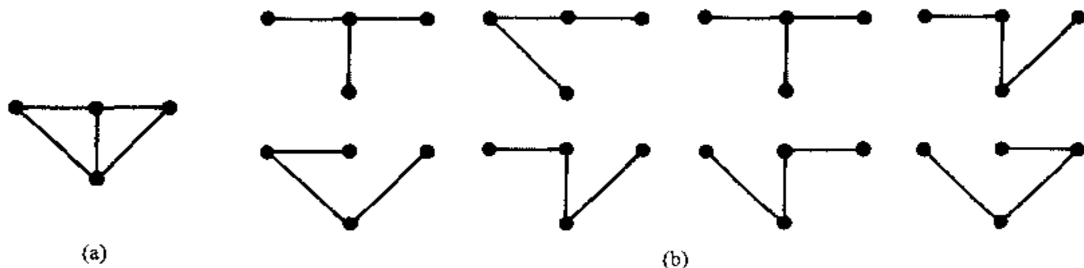


图 8－42

8.14　对于图 8－43(a)中的赋权图 G，求最小支撑树 T.

解 ☞　由于 G 有 $n=9$ 个顶点，故 T 必有 $n-1=8$ 条边. 应用算法 8.8A，即保持删除没有使 G 不连

通且有最大权的边，直至只剩下 $n-1=8$ 条边. 或应用算法 8.8B，即从 9 个点开始，保持添加不形成圈且有最小权的边，直至添加了 $n-1=8$ 条边. 两种方法都给出了最小支撑树，如图 8-43(b).

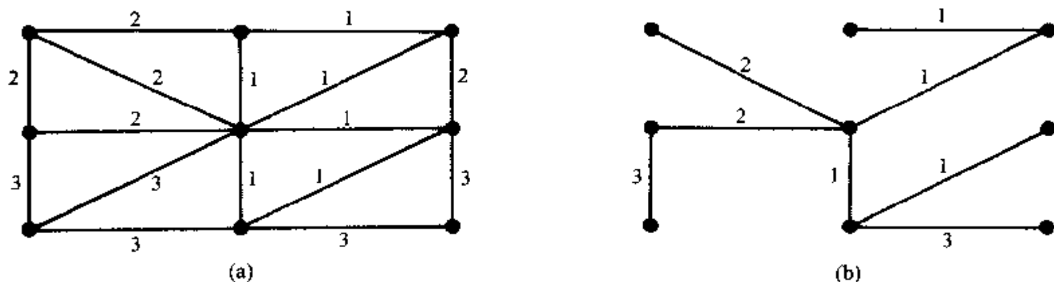


图 8-43

8.15 设 G 为多于一个顶点的图. 证明下列结论等价：(i) G 是树. (ii) 每对点恰由一条简单路连接. (iii) G 连通，但对 G 的任何边 e，$G-e$ 不连通. (iv) G 无圈，但若给 G 添加一条边则所得的图恰有一个圈.

证 ☞ (i)⇒(ii) 设 u 和 v 为 G 中的两点. 由于 G 为树，所以 G 是连通的，于是在 u 和 v 之间至少存在一条路. 由定理 8.37，u 和 v 之间只能有一条简单路. 否则 G 含有圈.

(ii)⇒(iii) 假如从 G 中删去边 $e=\{u,v\}$. 注意到 e 是从 u 到 v 的路，假设所得的图 $G-e$ 有从 u 到 v 的路 P，则 P 和 e 是两条不同的从 u 到 v 的路，与假设矛盾. 于是 $G-e$ 中 u 与 v 之间没有路，因此 $G-e$ 不连通.

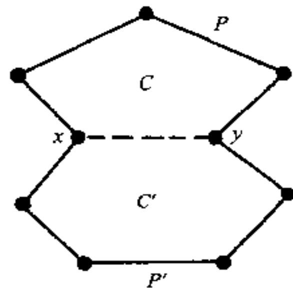


图 8-44

(iii)⇒(iv) 设 G 有一圈 C 含边 $e=\{u,v\}$. 由假设 G 连通，但 $G'=G-e$ 不连通，u 和 v 属于 G' 的两个不同的分支(问题 8.41). 这与 u 和 v 由一条 G' 中的路 $P=C-e$ 连接矛盾. 因而 G 是无圈的.

再令 x 和 y 为 G 的顶点，H 为由连接边 $e=\{x,y\}$ 到 G 所得到的图. 由于 G 是连通的，所以 G 中存在从 x 到 y 的路 P. 因此 $C=Pe$ 形成了 H 的圈. 假设 H 含有另一个圈 C'，由于 G 是无圈图，所以 C' 必含有边 e. 设 $C'=P'e$，那么 P 和 P' 为 G 中从 x 到 y 的两条简单路(见图 8-44). 由问题 8.37，G 含有一个圈，与 G 为无圈图矛盾. 因此，H 仅含有一个圈.

(iv)⇒(i) 因为给 G 添加一条边 $e=\{x,y\}$ 产生一个圈，所以顶点 x 与 y 在 G 中必定已是连通的. 因此 G 连通，且由假设 G 为无圈的，即 G 为树.

8.16 证明定理 8.6：设 G 为 $n\geqslant 1$ 个顶点的有限图，那么下列结论等价. (i) G 为树. (ii) G 无圈且有 $n-1$ 条边. (iii) G 连通且有 $n-1$ 条边.

证 ☞ 对 n 用归纳法证明. 对仅有一个顶点而没有边的图定理当然是对的. 即，定理对 $n=1$ 成立. 现假设 $n>1$，且定理对少于 n 个顶点的图成立.

(i)⇒(ii) 设 G 为树，则 G 是无圈的，因而只需证明 G 有 $n-1$ 条边，由问题 8.38，G 有度为 1 的顶点. 删去这个顶点以及它的边，便得到有 $n-1$ 个顶点的树 T. 定理对 T 成立，因此，T 有 $n-2$ 条边，于是 G 有 $n-1$ 条边.

(ii)⇒(iii) 设 G 是无圈的，且有 $n-1$ 条边，只需证明 G 连通. 假设 G 不连通，且有 k 个连通分支 $T_1,T_2,\cdots,T_k$，因为每个连通分支连通且无圈，所以都是树. 比方说 T_i 有 n_i 个顶点. 注意 $n_i<n$. 因此定理对 T_i 成立，于是 T_i 有 n_i-1 条边，因而

$$n=n_1-n_2+\cdots+n_k$$

且

$$n-1=(n_1-1)+(n_2-1)+\cdots+(n_k-1)-n_1+n_2+\cdots+n_k-k-n-k.$$

因此 $k=1$. 这与假设 G 不连通且有 $k>1$ 个分支矛盾. 因而 G 连通.

(iii)⇒(i) 设 G 连通且有 $n-1$ 条边，只需证明 G 无圈. 假设 G 有一个含边 e 的圈，删去 e 得到的图 $H=G-e$ 仍然连通. 但 H 有 n 个顶点和 $n-2$ 条边，这与问题 8.39 矛盾. 于是 G 无圈，因此为树.

平面图

8.17 若可能,画出图 8-45 中图的平面表示.

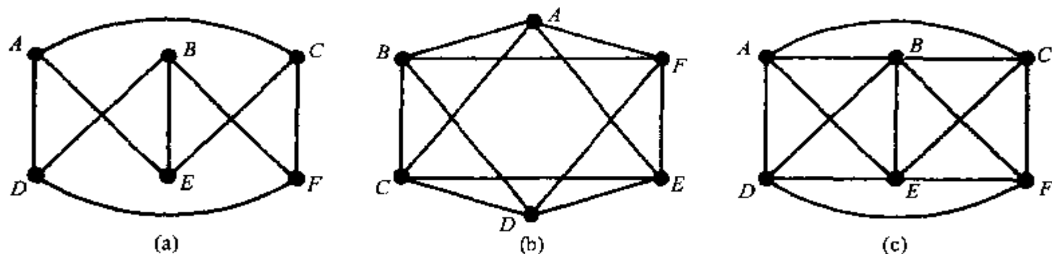


图 8-45

解 (a) 重画顶点 B 和 E 的位置,得到该图的平面表示,如图 8-46(a).

(b) 这不是星图 K_5,它有一平面表示,如图 8-46(b).

(c) 该图是非平面的.应用图 $K_{3,3}$ 为它的子图,如图 8-46(c).这里重画了顶点 C 和 F 的位置.

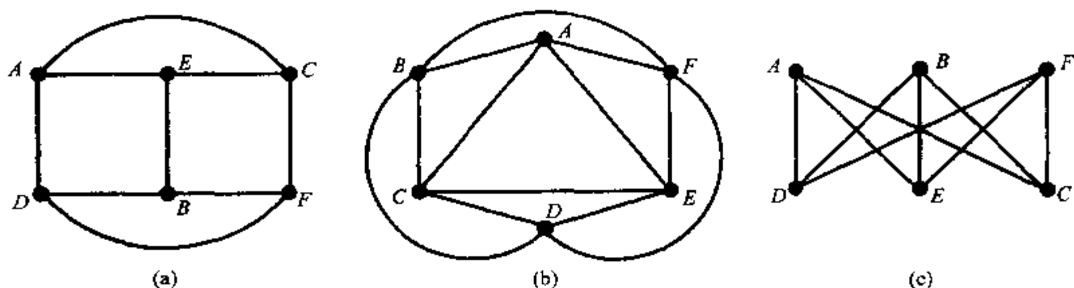


图 8-46

8.18 求出图 8-47 中各个地图的顶点数 V,边数 E 和区域数 R,并验证 Euler 公式.并求外部区域的度数.

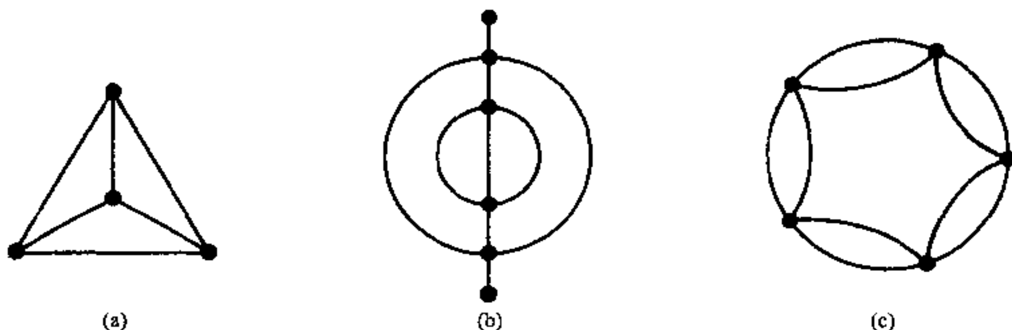


图 8-47

解 (a) $V=4,E=6,R=4$.因此,$V-E+R=4-6+4=2$. $d=3$.

(b) $V=6,E=9,R=5$.因此,$V-E+R=6-9+5=2$.由于两条边被计算两次,所以 $d=6$.

(c) $V=5,E=10,R=7$.因此,$V-E+R=5-10+7=2$. $d=5$.

8.19 求染图 8-47 中每个地图所需的最少颜色数.

解 (a) $n=4$.

(b) $n=3$.

(c) 仅需两种颜色,即 $n=2$.

8.20 证明定理 8.8(Euler):$V-E+R=2$.

证 假设连通地图 M 由单点 P 构成,见图 8-48(a).则 $V=1,E=0,R=1$.因此,$V-E+R=2$.

否则 M 可用下面两种构造法从单点构造出来.

(1) 添加新顶点 Q_2，且用一条边连接它到已有点 Q_1，这条边不穿过任何已有边，如图8-48(b).

(2) 用一条边连接两个已有的点. 这条边不穿过任何已有边，如图 8-48(c).

两种运算都不改变 $V-E+R$ 的值. 因此 M 与由单点构成的地图有相同的 $V-E+R$ 的值，即 $V-E+R=2$. 至此定理得证.

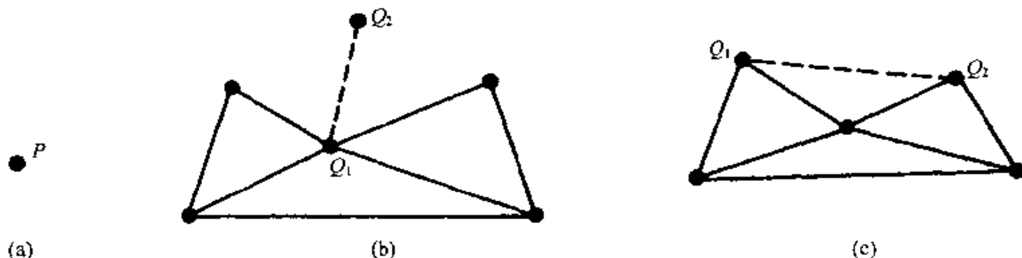


图 8-48

8.21 利用 Welch-Powell 算法给图 8-49 的图染色，并求这个图的色数 n.

解 ☞ 首先根据度递减的次序排列顶点得到下面的序列：

H,A,D,F,B,C,E,G. 相继地进行，用第一种颜色染顶点 H,B 和 G.（不能给 A,D 或 F 涂第一种颜色，因为它们都连接到 H，且不能给 C 或 E 涂第一种颜色，因为它们或连到 H 或连到 B.）对未染色的顶点相继进行，用第二种颜色染顶点 A 和 D. 剩下的顶点 F,C 和 E 涂第三种颜色. 于是色数 n 不超过 3. 然而在任何着色中，H,D 和 E 必须染不同的颜色，因为它们相互邻接. 因此 $n=3$.

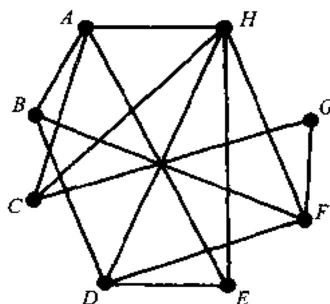


图 8-49

8.22 证明定理 8.11：对图 G 下面结论等价：(i) G 为 2-可着色的. (ii) G 为二部图. (iii) G 的每个圈有偶长度.

证 ☞ (i)⇒(ii) 设 G 为 2-可着色的，令 M 为涂第一种颜色的顶点集，N 为涂第二种颜色的顶点集. 那么 M 和 N 构成 G 的顶点的二部划分. 因为由于 $M(N)$ 中的顶点有相同的颜色，所以 $M(N)$ 中的顶点互不相邻.

(ii)⇒(iii) 设 G 为二部图，M,N 为 G 的顶点的二部划分. 比方说，若一个圈开始于 M 的点 u，那么它到 N 的点，再到 M 的点，再到 N 的点，等等. 因此当该圈回到 u 时，它必具有偶长度，即 G 的每个圈有偶长度.

(iii)⇒(i) 最后，假设 G 的每个圈有偶长度，在每个连通分支中取一点，并染第一种颜色，比方说红色. 然后如下相继地染所有的点：若一点染红色，则任何连接到它的点染第二种颜色，比方说蓝色. 若一点染蓝色，则任何连接到它的点染红色，因为每个圈有偶长度，所以没有相邻的点涂相同的颜色. 因此，G 为 2-可着色的. 定理得证.

8.23 设 G 为至少 3 个顶点的有限连通平面图. 证明 G 至少有一个不超过 5 度的顶点.

证 ☞ 设 p 为图 G 的顶点数，q 为 G 的边数，并假设对 G 的每个顶点 u，有 $\deg(u)\geqslant 6$. 但 $2q$ 为 G 的顶点的度之和(定理 8.1)，因此 $2q\geqslant 6p$.

于是

$$q\geqslant 3p>3p-6$$

与定理 8.9 矛盾，因而 G 的某个点度至多为 5.

8.24 证明定理 8.12：平面图 G 是 5-可着色的.

证 ☞ 对 G 的顶点数 p 用归纳法证明. 若 $p\leqslant 5$，则定理明显成立. 假设 $p>5$，且定理对少于 p 个顶点的图成立. 由前面的问题，G 有一个顶点 v 使得 $\deg(v)\leqslant 5$. 由归纳假设，$G-v$ 是 5-可着色的. 假定一个这样的着色. 如果邻接到 v 的顶点用了少于 5 种颜色，那么简单地用剩下的颜色之一涂 v 便得到 G 的 5-着色. 剩下的情形是 v 邻接到 5 个顶点，且它们涂了不同的颜色，比方说，关于 v 逆时针方向的 5 个顶点为 $v_1,v_2,\cdots,v_5$. 且分别染颜色 $c_1,c_2,\cdots,c_5$.（见图 8-50.）

现考虑 G 的由染 c_1 和 c_3 颜色的点生成的子图 H，注意到 H 含有 v_1 和 v_3. 若 v_1 和 v_3 属于 H 的不同分支. 则在含 v_1 的分支中交换颜色 c_1 和 c_3 并不破坏 $G-v$ 的着色. 于是 v_1 和 v_3 染 c_3，c_1 可用来染 v，从而有 G 的 5-着色. 另一方面，假设 v 和 v_1 在 H 的同一个分支中. 那么存在一条从 v_1 到 v_3 的路 P，P 的顶点或者染 c_1 或者染 c_3，P 与边 $\{v,v_1\}$ 和 $\{v,v_3\}$ 一起构成一个圈. 这个圈或者围住了 v_2 或者围住了 v_4. 现考虑由染 c_2 或 c_4 的顶点生成的子图 K，由于 C 围住了 v_2 或 v_4，但不是两个，所以 v_2 和 v_4 必属于 K 的不同分支，由此在含 v_2 的分支中交换颜色 c_2 和 c_4 并不破坏 $G-v$ 的着色. 因此 v_2 和 v_4 染颜色 c_4，可选 c_2 染 v. 从而得到 G 的 5-着色. 因此 G 为 5-可着色的，定理得证.

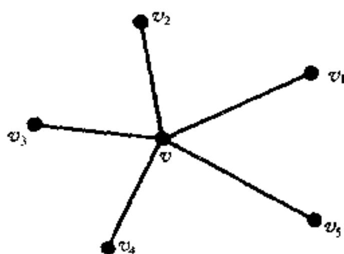


图 8-50

图的序列表示

8.25 求图 8-51 中各图的邻接矩阵 $A=[a_{ij}]$.



图 8-51

解 若有 n 条边 $\{v_i,v_j\}$，则设 $a_{ij}=n$，否则设 $a_{ij}=0$，因此

$$(a)\quad A=\begin{bmatrix}0&1&0&1\\1&0&1&1\\0&1&0&1\\1&1&1&0\end{bmatrix};\qquad (b)\quad A=\begin{bmatrix}1&0&0&1\\0&0&2&1\\0&2&0&0\\1&1&0&1\end{bmatrix}.$$

[因为(a)没有重边，也没有环，所以 A 中的值或为 0 或为 1，且对角线上元素为 0.]

8.26 对应于每个邻接矩阵画出图 G.

$$(a)\quad A=\begin{bmatrix}0&1&0&1&0\\1&0&0&1&1\\0&0&0&1&1\\1&1&1&0&1\\0&1&1&1&0\end{bmatrix};\qquad (b)\quad A=\begin{bmatrix}1&3&0&0\\3&0&1&1\\0&1&2&2\\0&1&2&0\end{bmatrix}.$$

解 (a) 因为 A 为 5 阶方阵，所以 G 有 5 个顶点，设为 $v_1,v_2,\cdots v_5$. 当 $a_{ij}=1$ 时画一条从 v_i 到 v_j 的边，这个图如图 8-52(a).

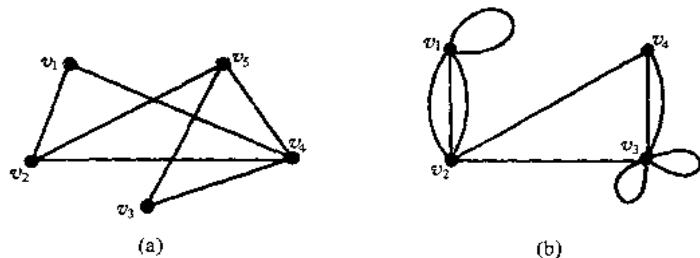


图 8-52

(b) 因为 A 为 4 阶方阵，所以 G 有 4 个顶点，设为 $v_1,\cdots,v_4$. 当 $a_{ij}=n$ 时，画 n 条从 v_i 到 v_j 的边，当 $a_{ii}=n$ 时，在 v_i 处画 n 个环. 这个图如图 8－52(b).

8.27 考察图 8－53 中的赋权图 G，假设顶点存贮在数组 DATA 中，

$$\text{DATA}: A,\ B,\ C,\ X,\ Y.$$

求图 G 的赋权矩阵 $W=(w_{ij})$.

解 ☞ 根据它们在组 DATA 中的存贮，给顶点标号，即 $v_1=A, v_2=B,\cdots,v_5=Y$. 置 $w_{ij}=w$，其中 w 为从 v_i 到 v_j 的边的权. 于是，

$$W=\begin{bmatrix}0&6&0&4&1\\6&0&5&0&8\\0&5&0&0&2\\4&0&0&0&3\\1&8&2&3&0\end{bmatrix}.$$

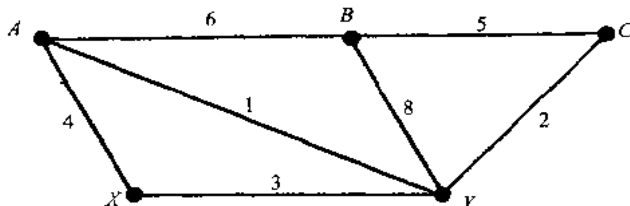


图 8－53

图的链表示

8.28 具有顶点 $A,B,\cdots,F$ 的图 G 用图 8－54 的点文件和边文件链表示存贮.

(a) 按在存贮中出现的次序列出顶点.

(b) 求 G 的每个顶点 v 的邻接表 adj(v).

点文件

START [4]

	1	2	3	4	5	6	7	8
VERTEX	B		F	D	A		C	E
NEXT-V	3		5	1	8		0	7
PTR	9		4	7	6		5	12

边文件

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ADJ	4	4	1	8	8	1	5	3	5	8	4	7		
NEXT	8	0	10	0	0	2	3	0	11	0	0	1		

图 8－54

解 ☞ (a) 因为 START＝4，所以列表以顶点 D 开始，NEXT-V 告诉我们到 1(B)，再到 3(F)，再到 5(A)，再到 8(E)，再到 7(C)，即

$$D,\ B,\ F,\ A,\ E,\ C.$$

(b) 这里 adj(D)＝[5(A)，1(B)，8(E)]，特别地，PTR[4(D)]＝7 和 ADJ[7]＝5 告诉我们 adj(D)以 A 开始. 于是 NEXT[7]＝3 和 ADJ[3]＝1(B)告诉我们 B 为 adj(D)中的后继点. 于是 NEXT[3]＝10 和 ADJ[10]＝8(E)告诉我们 E 为 adj(D)中的后继点. 然而 NEXT[10]＝0 告知 D 中没有更多的邻点，类似地，

$$\text{adj}(B)=[A,D],\ \text{adj}(F)=[E],\ \text{adj}(A)=[B,D],$$
$$\text{adj}(E)=[C,D,F],\ \text{adj}(C)=[E].$$

换句话说，G 的邻接结构如下：

$$G=[A{:}B,D;\ B{:}A,D;\ C{:}E;\ D{:}A,B,E;\ E{:}C,D,F;\ F{:}E].$$

8.29 画出其链表示为图 8－54 的图 G.

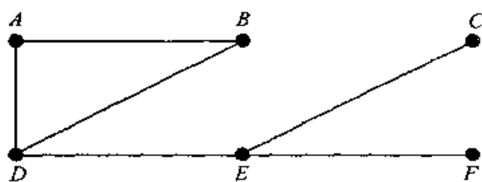


图 8-55

解 利用问题 8.28(a)中得到的顶点列表以及问题 8.28(b)中得到的邻接表可画出图 G,如图 8-55.

8.30 给出(a)　图 8-31,(b)　图 8-32 中的图 G 的邻接结构(AS).

解 图 G 的邻接结构由点的邻接表构成,这里用冒号":"分隔点与其邻接表,并用分号";"来分隔不同的列表.于是:

(a) $G=[A{:}B,C,D;\ B{:}A,C,E;\ C{:}A,B,D,E;\ D{:}A,C;\ E{:}B,C]$.

(b) $G=[A{:}B,D;\ B{:}A,C,E;\ C{:}B,E,F;\ D{:}A,E;\ E{:}B,C,D,F;\ F{:}C,E]$.

图算法

8.31 考虑图 8-56 中的图 G. (a) 求 G 的邻接结构. (b) 求由 A 开始用 DFS(深度优先查找)算法检查 G 的顶点次序.

解 (a) 如下列出每个顶点的邻点:

$G=[A{:}B,C,D;\ B{:}A,E;\ C{:}A;\ D{:}A,F;\ E{:}B,F,H;\ F{:}D,E,G;\ G{:}F,H;\ H{:}E,G]$.

(b) 在 DFS 算法中,堆栈的第一个顶点 N 检查,且 N 的邻点(前面没有检查过)被放到堆栈上.最初,起始点 A 被放到堆栈上.下面给出了堆栈的等候表的序列以及正在检查的顶点:

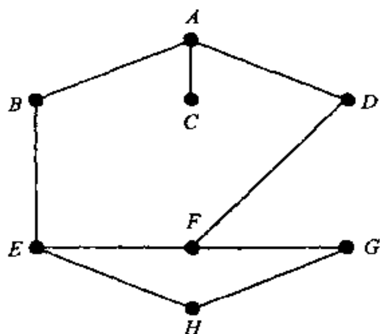


图 8-56

顶点		A	B	E	F	D	G	H	C
堆栈	A	BCD	ECD	FHCD	DGHCD	GHC	HHC	C	

换句话说,顶点按 A,B,E,F,D,G,H,C 的次序检查.

8.32 求从顶点 A 开始,用 BFS(广度优先查找)算法,检查图 8-56 中的图 G 的顶点的次序.

解 在用 BFS 算法时,队列的第一个顶点被检查,且 N 的邻点(前面未出现)被添加到队列中,最初,起始点 A 被指派到队列中.下面给出队列中等候列表的序列以及正在检查的点:

顶点		A	B	C	D	E	F	H	G
队列	A	BCD	CDE	DE	EF	FH	HG	G	

换句话说,顶点以 A,B,C,D,E,F,H,G 的次序检查.

补　充　题

图术语

8.33 考虑图 8-57 中的图.求:(a) 每个顶点的度(并验证定理 8.1);(b) 从 A 到 G 的所有简单路;(c) 从 B 到 C 的所有迹(不同的边);(d) 从 A 到 C 的距离 $d(A,C)$;(d) G 的直径 diam(G).

8.34 考虑图 8-57 中的图.若有,求:(a) 所有的圈;(b) 所有割点;(c) 所有的桥.

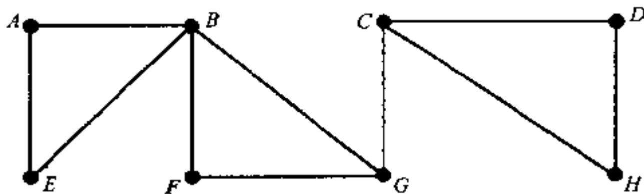


图 8 - 57

8.35 考虑图 8 - 57 中的图. 求由(a) $V'=\{B,C,D,E,F\}$,(b)$V'=\{A,C,E,G,H\}$,(c) $V'=\{B,D,E,H\}$,(d) $V'=\{C,F,G,H\}$生成的子图 $H(V',E')$. 其中哪些同构? 哪些同胚?

8.36 考虑图 8 - 58 中的多重图 G. (a) 其中哪些连通? 若不连通,求连通分支数. (b) 哪些无圈(没有圈)? 若不是,求圈的数. (c) 哪些无环(没有环)? (d) 哪些是(简单)图?

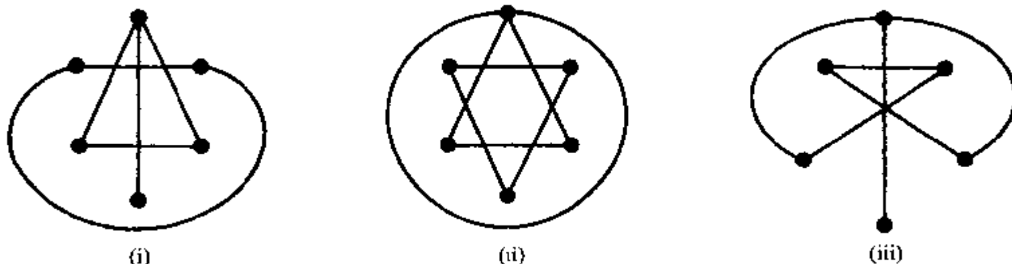


图 8 - 58

8.37 设图 G 有从顶点 u 到 v 两条不同的路,证明 G 有圈.

8.38 设 G 为至少一条边的有限无圈图,证明 G 至少有两个 1 度顶点.

8.39 证明 n 个顶点的连通图 G 必定至少有 $n-1$ 条边.

8.40 求具有 4 个顶点的连通图的个数(画出来).

8.41 设 G 为连通图,证明

(a) 若 G 含有经过 e 的圈,则 $G-e$ 仍连通.

(b) 若 $e=\{u,v\}$为使 $G-e$ 不连通的一条边. 则 u 和 v 属于 $G-e$ 的不同的分支.

8.42 对图 G 考虑下面两步:(1) 删除一条边. (2) 删除一个顶点以及含那个顶点的所有边. 证明:有限图 G 的每个子图 H 可由一系列这两步得到.

可旅行图,Euler 回路与 Hamilton 回路

8.43 考虑图 8 - 59 中的每个图 G. 若有的话,求一条 Euler 路(可旅行路). 若没有,说明为什么.

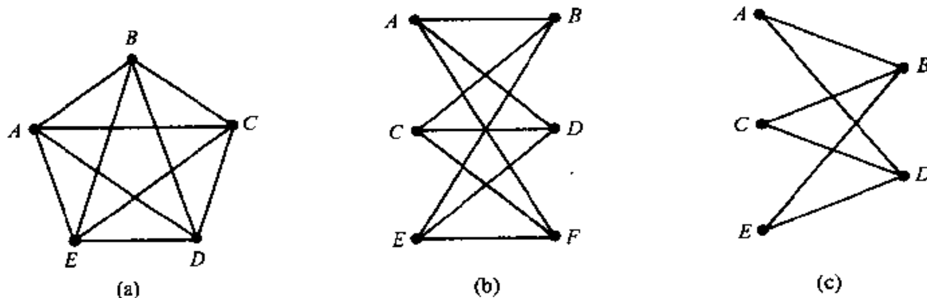


图 8 - 59

8.44 考虑图 8 - 59 中的每个图 G. 若有,求一条 Hamilton 路或 Hamilton 回路. 若没有,说明为什么.

8.45 求图 8 - 59(a)中图的 Hamilton 回路的数目.

8.46 设 G 和 G^* 是同胚图. 证明 G 是可旅行的(Euler 图)当且仅当 G^* 是可旅行的(Euler 图).

特殊图

8.47 画两个 8 个顶点的 3 - 正则图.

8.48 画两个 9 个顶点的 3-正则图.

8.49 考虑完全图 K_n.

(a) 求 K_n 的边数 m.

(b) 求 K_n 中每个顶点的度数.

(c) 若 K_n 是可旅行的,求 n 的值.

(d) 若 K_n 是正则的,求 n 的值.

8.50 考虑完全二部图 $K_{m,n}$.

(a) 求 $K_{m,n}$ 的直径.

(b) 求可旅行的那些 $K_{m,n}$.

(c) 图 $K_{m,n}$ 中哪些同构? 同胚呢?

树

8.51 画出不多于 5 个顶点的所有树.

8.52 求 7 个顶点的树的个数.

8.53 求图 8-60 中支撑树的个数.

8.54 求图 8-61 中最小支撑树的权.

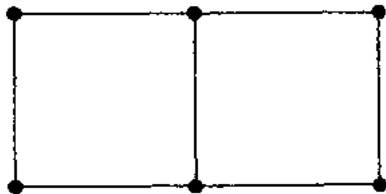


图 8-60

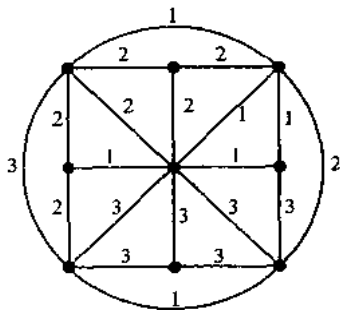


图 8-61

8.55 证明树是二部图.

8.56 什么样的完全二部图 $K_{m,n}$ 是树?

平面图,地图,着色

8.57 若可能,画出图 8-62 中每个图的平面表示. 否则证明它有一个同胚于 K_5 或 $K_{3,3}$ 的子图.

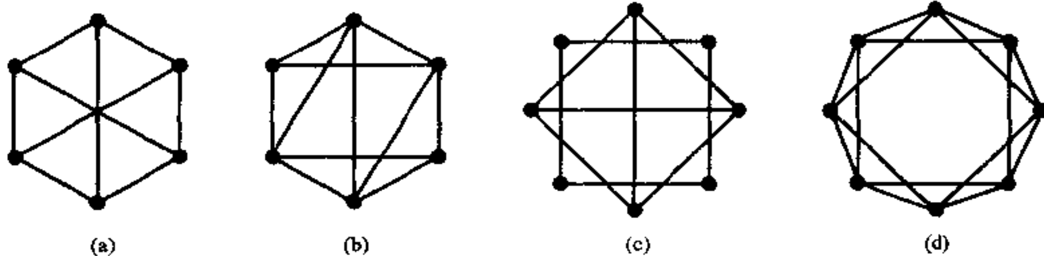


图 8-62

8.58 对图 8-63 中的地图,求每个区域的度数,并验证区域的度和等于边数的两倍.

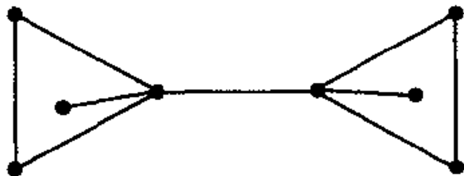


图 8-63

8.59 计数图 8－64 中每个地图的顶点数 V，边数 E 以及区域数 R．并验证 Euler 公式．

8.60 求给图 8－64 中每个地图的区域染色所需的最小颜色数．

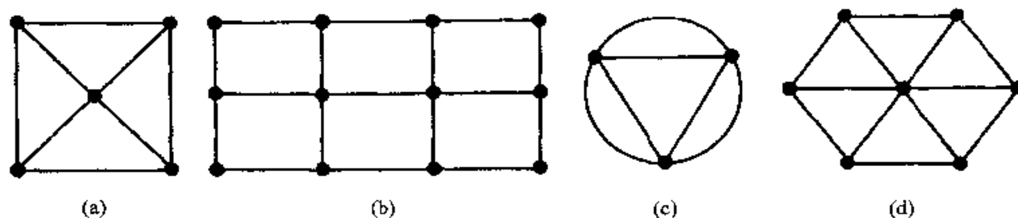


图 8－64

8.61 画出图 8－64 中各个地图的对偶地图．

8.62 用 Welch-Powell 算法给图 8－65 中的每个图染色，求它们的色数 n．

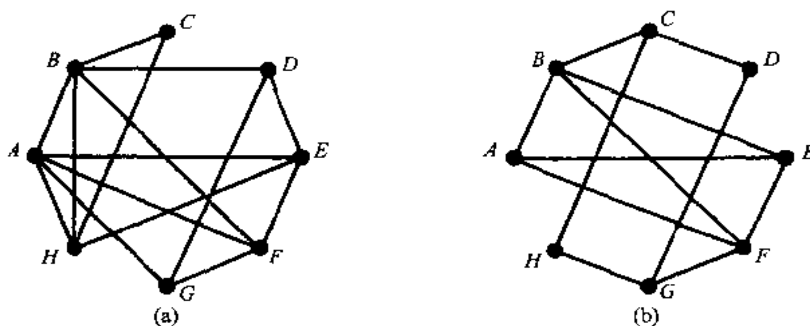


图 8－65

图的序列表示

8.63 求图 8－66 中每个图的邻接矩阵 A．

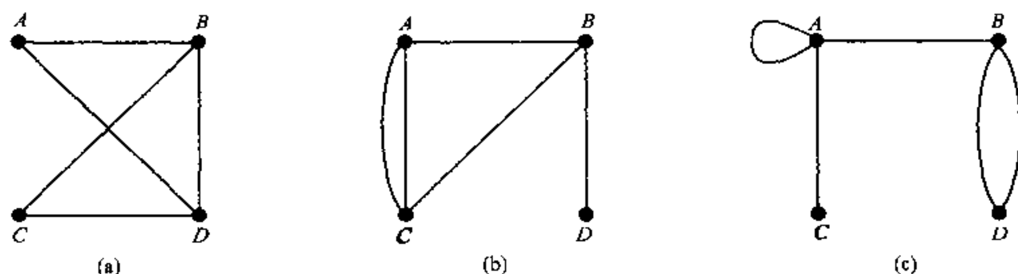


图 8－66

8.64 根据下面的邻接矩阵画出多重图．

$$(a)\quad A=\begin{bmatrix}0&2&0&1\\2&1&1&1\\0&1&0&1\\1&1&1&0\end{bmatrix};\quad (b)\quad A=\begin{bmatrix}0&1&1&2\\1&0&0&0\\1&0&0&2\\ &0&2&2\end{bmatrix}.$$

8.65 设图 G 为二部图．证明可以对 G 的顶点排序使得它的邻接矩阵 A 有下列形式

$$A=\begin{bmatrix}0&B\\C&0\end{bmatrix}.$$

图的链表示

8.66 设图 G 如图 8－67 存贮．

(a) 按顶点存贮的次序列出顶点．

(b) 求 G 的邻接结构，即求 G 的每个顶点 v 的邻接表 adj(v)．

8.67 给出图 8－59 中每个图 G 的邻接结构(AS)．

点文件

START 7

	1	2	3	4	5	6	7	8
VERTEX	C		F	E	A		B	D
NEXT-V	0		5	1	8		3	4
PTR	2		11	6	12		4	1

边文件

	1	2	3	4	5	6	7	8	9	10	11	12
ADJ	7	7	4	5		7	1		8	3	1	7
NEXT	0	10	0	7		0	9		3	0	0	0

图 8-67

8.68 图 8-68 给出了图 G,它代表 6 个城市 $A,B,\cdots,F$,由 7 条标上 22,33,…,88 的高速公路连接. 证明 G 可用链表示存贮,具有城市与标号高速公路分类组.(注意 VERTEX 是一个分类组,因此字段 NEXT-V 是不必要的.)

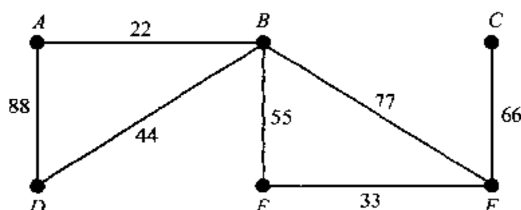


图 8-68

图算法

8.69 考虑图 8-57 中的图 G.

(a) 求 G 的邻接结构.

(b) 利用开始于(i) 顶点 C,(ii)顶点 B 的 DFS(深度优先查找)算法,求顶点检查的次序.

8.70 利用开始于(a) 顶点 C,(b) 顶点 B 的 BFS(广度优先查找)算法,求图 8-57 中图 G 顶点检查的次序.

补充题答案

8.33 (a) 2,4,3,2,2,2,3,2; (b) $ABG,ABFG,AEBG,AEBFG$; (c) $BGC,BFGC,BAEBGC,BAEBFGC$; (d) 3; (e) 4.

8.34 (a) $ABEA$, $BFGB$, $CDHC$; (b) B,C,G; (c) 仅$\{C,G\}$.

8.35 (a) $E'=\{BE,BF,CD\}$; (b) $E'=\{AE, CH, GC\}$; (c) $E'-\{BE, DH\}$; (d) $E'=\{FG, GC,CH\}$. 又(a)和(b)同构,(a),(b)和(c)同胚.

8.36 (a) (iii) 连通,(i)和(ii)有两个连通分支. (b) 没有. (c) (i)和(iii). (d) (iii).

8.38 提示:考虑极大简单路 α,证明其端点的度为 1.

8.40 其中有 5 个,如图 8-69.

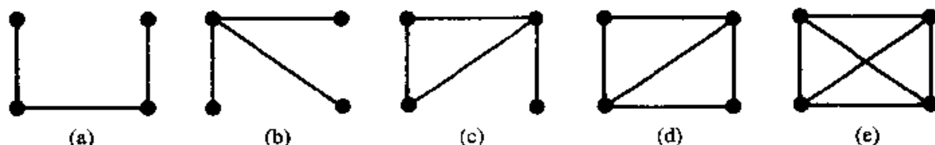


图 8-69

8.42 首先删除在 G 中但不在 H 中的所有边,然后删除在 G 中但不在 H 中的所有顶点.

8.43 (a) 由于所有顶点为偶点,所以是 Euler 图: $ABCDEACEBDA$. (b) 没有,因为 6 个顶点都为奇点. (c) 开始于 B 结束于 D 的(或反过来)的 Euler 路: $BADCBED$.

8.44 (a) $ABCDEA$. (b) $ABCDEFA$. (c) 有 Hamilton 路 ABCDE,但没有 Hamilton 回路. 因为在包含所有

顶点的任何闭路中，B 或 D 必定访问 2 次.

8.45 12.

8.46 提示：添加一个点剖分一条边并不改变原来点的度数，仅增加了一个偶度点.

8.47 图 8-70 中的两个 3-正则图不同构，因为 (b) 有 5-圈，但(a) 没有.

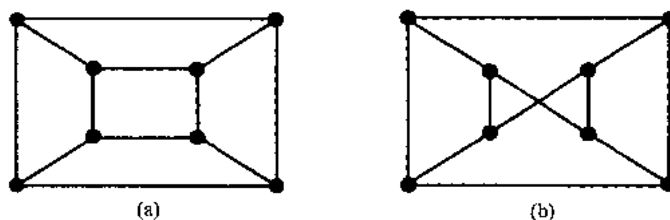


图 8-70

8.48 没有，s 个顶点的 r-正则图的度和等于 rs，但它必须为偶数.

8.49 (a) $m=C(n,2)=n(n-1)/2$. (b) $n-1$. (c) $n=2$ 或 n 为奇数. (d) 所有的 n.

8.50 (a) $\operatorname{diam}(K_{1,1})=1$，所有其他的 $K_{m,n}$ 直径为 2.

(b) $K_{1,1}$，$K_{1,2}$ 与所有 m,n 为偶数的 $K_{m,n}$.

(c) 没有同构的，只有 $K_{1,1}$ 与 $K_{1,2}$ 同胚.

8.51 如图 8-71，有 8 个这样的树，有一个顶点而没有边的图是平凡树.

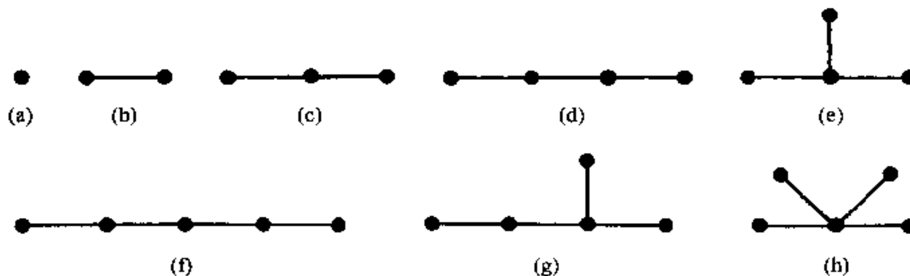


图 8-71

8.52 10.

8.53 15.

8.54 $1+1+1+1+1+2+2-3=12$.

8.56 $m=1$.

8.57 只有(a)为非平面，且 $K_{3,3}$ 为一个子图.

8.58 外部区域的度为 8，其他两个区域度为 5.

8.59 (a) 5,8,5. (b) 12,17,7. (c) 3,6,5. (d) 7,12,7.

8.60 (a) 3. (b) 3. (c) 2. (d) 3.

8.61 如图 8-72.

8.62 (a) $n=3$; (b) $n=4$.

8.63 (a) $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$; (b) $\begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$; (c) $\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ & 2 & 0 & 0 \end{bmatrix}$.

8.64 如图 8-73.

8.65 设 M 和 N 为确定二部图 G 的两个不相交的顶点集. 先排 M 中顶点序，再排 N 中的顶点序.

8.66 (a) B, F, A, D, E, C.

(b) $G=[A:B;\ B:A,\ C,\ D,\ E;\ C:F;\ D:B;\ E:B;\ F:C]$.

8.67 (a) 每个顶点邻接到其他 4 个顶点.

(b) $G=[A:B,D,F;\ B:A,C,E;\ C:B,D,F;\ D:A,C,E;\ E:B,D,F;\ F:A,C,E]$.

(c) $G=[A:B,D;\ B:A,C,E;\ C:B,D;\ D:A,C,E;\ E:B,D]$.

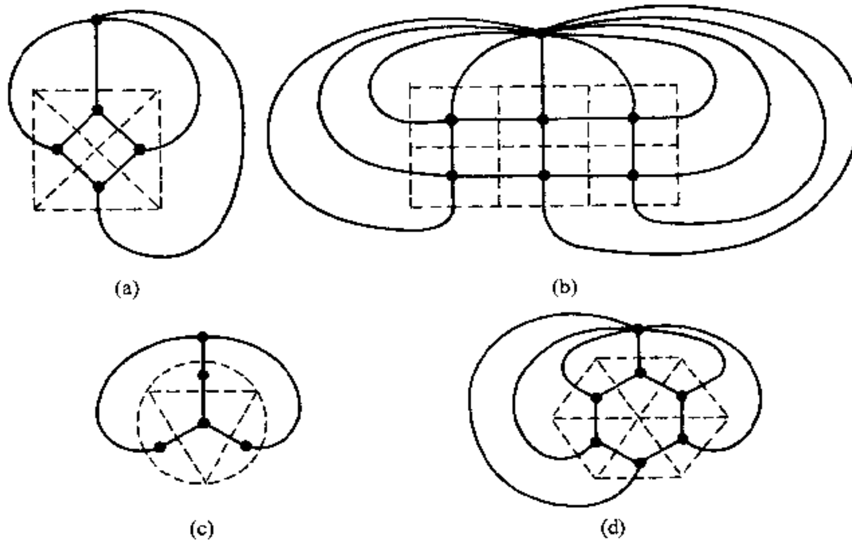


图 8－72

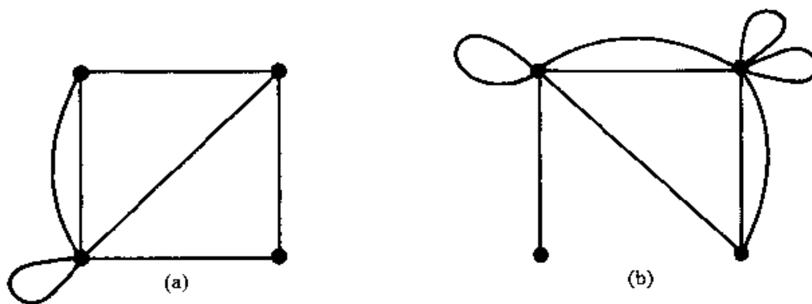


图 8－73

8.68 如图 8－74.

点文件

	1	2	3	4	5	6	7	8
VERTEX	*A*	*B*	*C*	*D*	*E*	*F*		
PTR	1	2	9	14	8	12		

边文件

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
NUMBER	22	22	33	33	44	44	55	55	66	66	77	77	88	88	
ADJ	2	1	6	5	4	2	5	2	6	3	6	2	4	1	
NEXT	13	5	0	0	7	0	11	3	0	4	0	10	0	6	

图 8－74

8.69 (a) $G=[A:B,E;\ B:A,E,F,G;\ C:D,G,H;\ D:C,H;\ E:A,B;\ F:B,G;\ G:B,C,F;\ H:C,D]$.

(b) (i) C,D,H,G,B,A,E,F; (ii) B,A,E,F,G,C,D,H.

8.70 (a) C,D,G,H,B,F,A,E; (b) B,A,E,F,G,C,D,H.

第九章　有 向 图

9.1　引　言

有向图是边带有一个方向的图.在诸如数字计算机或流系统等各种动态系统中,这样的图常常更有用.然而,增加了这个特征之后,确定图的某些性质将更加困难.即处理这样的图也许类似于在具有许多单行线的城市中旅行.

有向图在第三章研究关系时已经出现,人们可以将某些有向图看成(二元)关系.基于此,某些教材在关系的背景下讨论有向图.事实上这里将给出一个有效算法来求关系的传递闭包.

本章给出有向图的基本定义和性质.许多定义类似于前一章有关(无向)图的定义.然而,为教学的原因,本章的主要部分将不依赖于前一章独立.

9.2　有向图

有向图由两个对象构成:

(i) 其元素称为顶点的集合 V.

(ii) 称为弧或有向边或简称为边的有序顶点对(u,v)的集合 E.

当强调 G 的两个部分时,记为 $G(V,E)$.也分别用 $V(G)$和 $E(G)$表示图 G 的顶点集和边集(若非特别说明,由上下文将可说明图 G 是否为有向图.)

设 $e=(u,v)$为有向图 G 的有向边.则使用下列术语:

(a) e *起于* u,*终于* v.

(b) u 为 e 的*始点*,v 为 e 的*终点*.

(c) v 为 u 的*后继*.

(d) u *邻接到* v,v *从* u *邻接*.

若 $u=v$,则 e 称为*环*.

顶点 u 的所有后继的集合是重要的.它的记号和定义如下:

$$\mathrm{succ}(u)=\{v\in V:\text{存在}(u,v)\in E\}.$$

称为 u 的*后继表*或*邻接表*.

有向图 G 在平面上的表示称为有向图 G 的*表示*.即,G 的每个点 u 用一个点(或小圆圈)表示,而每条(有向)边用一个从 e 的起点 u 到终点 v 的箭头或有向曲线表示.通常用一个示意图示给出的有向图,而不再详细列出它的顶点与边.

若有向图 G 的顶点与/或边用某种数据标号,则 G 称为*标号有向图*.

有向图 $G(V,E)$的顶点集和边集是有限的,则称 $G(V,E)$为*有限的*.

例 9.1　(a) 考虑画在图 9－1 中的有向图 G.它由下面的 4 个顶点和 7 条边构成:

$$V(G)=\{A,B,C,D\},$$

$$E(G)=\{e_1,\cdots,e_7\}=\{(A,D),(B,A),(B,A),(D,B),(B,C),(D,C),(B,B)\},$$

边 e_2 和 e_3 称为*平行的*,因为它们都起于 B 终于 A,边 e_7 是一个环,因为它起于也终于 B.

(b) 假设三个男孩 A,B,C 相互扔球,使得 A 总是扔给 B,但 B,C 正好都扔给 A,且与 B 与 C 之间相互扔球的可能性相同.图 9－2 解释了这个动态系统,其中每条边标上各自的概率,即 A 扔球给 B 的概率为 1,B 扔球给 A 与 C 的概率都为$\frac{1}{2}$,C 扔球给 A 和 B 的概率都为$\frac{1}{2}$.

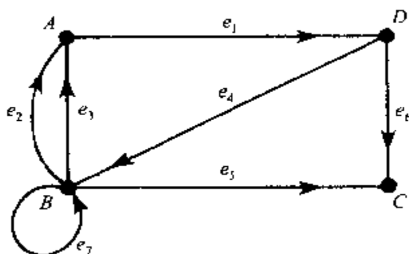


图 9-1

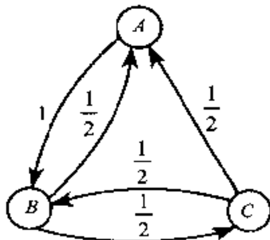


图 9-2

子图

设$G=G(V,E)$为有向图,V'为G的顶点集V的子集,又设E'为E的子集,使得E'中边的端点都属于V',则$H(V',E')$为有向图,称为G的子图.特别地,若E'含有E中其端点属于V'的所有边.则$H(V',E')$称为G的由V'生成的子图.例如,考虑图9-1中的图$G=G(V,E)$.设

$$V'=\{B,C,D\}\text{和}E'=\{e_4,e_5,e_6,e_7\}=\{(D,B),(B,C),(D,C),(B,B)\},$$

则$H(V',E')$为G的由顶点集V'生成的子图.

9.3 基本定义

本节讨论有向图中顶点的度、路及连通度等问题.

度

设G为有向图.G的顶点v的*出度* outdeg(v)为起始于v的边数,v的*入度* indeg(v)为终于v的边数,由于每条边起于、终于一个点,因此立即有下面的定理.

定理 9.1 有向图G的顶点出度之和等于顶度的入度之和,都等于G的边数.

入度为0的顶点称为*发点*,出度为0的顶点称为*收点*.

例 9.2 考虑图9-1中的图G.有

$$\text{outdeg}(A)=1,\quad \text{outdeg}(B)=4,\quad \text{outdeg}(C)=0,\quad \text{outdeg}(D)=2,$$
$$\text{indeg}(A)=2,\quad \text{indeg}(B)=2,\quad \text{indeg}(C)=2,\quad \text{indeg}(D)=1.$$

正如所料,出度之和等于入度之和,都等于边数7.顶点C为收点,因为没有边起始于C.该图没有发点.

路

设G为有向图.则路、简单路、迹与圈的概念都从无向图中平移过来,只是边的方向必须与路的方向一致,特别地,

(i) G中*(有向)路* P为顶点与有向边的交错序列,如

$$P=(v_0,e_1,v_1,e_2,v_2,\cdots,e_n,v_n)$$

满足e_i起于v_{i-1},终于v_i.若不引起混淆,可用它的顶点序列或边序列表示P.

(ii) 路P的*长度*是n,为它的边数.

(iii) *简单路*是顶点不相同的路.*迹*是边不相同的路.

(iv) *闭路*有相同的起点与终点.

(v) *支撑路*含有G的所有顶点.

(vi) *圈*(或*回路*)是具有不同顶点的闭路(除了起点与终点外).

(vii) *半路*是一条路,只是边e_i可能起于v_{i-1}或v_i,而终于另一点.*半迹*与*半简单路*可类似地定义.

如果存在一条从u到v的路,那么就称顶点v从顶点u *可达*.若v从u可达,则(去掉多余

的边)必存在一条从 u 到 v 的简单路.

例 9.3 考虑图 9-1 中的图 G.

(a) 序列 $P_1=(D,C,B,A)$是半路,但不是路,因为(C,B)不是一条边,即 $e_5=(C,B)$ 的方向与 P_1 的方向不一致.

(b) 序列 $P_2=(D,B,A)$是一条从 D 到 A 的路. 因为(D,B)与(B,A)是边,因此,A 从 D 可达.

连通度

有向图 G 有三种连通度:

(i) G 为*强连通的*或*强的*,如果对 G 的任意点对 u 和 v 都存在从 u 到 v 的路以及从 v 到 u 的路,即每个点从其他点可达.

(ii) G 为*单侧连通的*或*单侧的*,如果对 G 的每对顶点 u 和 v,存在一条从 u 到 v 的路或存在一条从 v 到 u 的路,即其中一点从另一点可达.

(iii) G 为*弱连通的*或*弱的*,如果 G 的任一对顶点 u 和 v 之间总存在一条半路.

设 G' 为从有向图 G 得到的(无向)图,即将 G 的所有边视为无向边得到的图. 显然,G 弱连通当且仅当图 G' 连通.

注意到强连通蕴含了单侧连通,而单侧连通又蕴含着弱连通. 称 G 为*严格单侧连通*是指它是单侧的,但不是强的;称 G 为*严格弱的*是指它是弱的,但不是单侧的.

连通度可用支撑路来刻画.

定理 9.2 设 G 为有限有向图,则

(i) G 是强的当且仅当 G 有一条闭支撑路.

(ii) G 是单侧的当且仅当 G 有一条支撑路.

(iii) G 是弱的当且仅当 G 有一条支撑半路.

例 9.4 考虑图 9-1 中的图 G. 它是弱连通的,因为基础无向图是连通的. 没有从 C 到其他任何点的路(即 C 为收点),因此 G 不是强连通的. 然而 $P=(B,A,D,C)$为支撑路,故 G 为单侧连通的.

许多应用中会出现有收点和发点的图(例如,流图表与网络),下面给出存在这些点的充分条件.

定理 9.3 设有限有向图 G 是无圈的,即不含(有向)圈,则 G 有收点和发点.

证明 设 $P=(v_0,v_1,\cdots,v_n)$为具有最大长度的简单路,它是存在的,因为 G 是有限的. 那么最后顶点 v_n 为收点,否则有一条边(v_n,u)或者扩展 P,或者形成一个圈,此时对某 i,有 $u=v_i$,类似地,第一个顶点 v_0 为发点.

9.4 有根树

回忆树图是连通无圈图,即没有圈的连通图. *有根树* T 是一个有称为*树根*的指定顶点 r 的树图. 由于存在惟一的简单路从根 r 到 T 的任何其他顶点 v,因此,这便确定了 T 中各边的方向. 于是 T 可以看成一个有向图. 注意到任何树都可以变成有根树,只需简单地选取其中一个顶点作为树根即可.

考虑有根 r 的有根树 T,从根 r 到任何顶点 v 的路的长度称为 v 的*层次*(或*深度*)记,顶点层次的最大值称为该树的深度. 除了根 r 外,度为 1 的那些顶点称为 T 的*树叶*,从一个顶点到一个树叶的有向路称为一个*支*.

画有根树 T 时常把根画在树的顶上,图 9-3 给了一个根为 r 且有 10 个其他顶点的有根树 T. 该树有 5 个树叶,d,f,h,i 和 j,注意到:

$$\text{level}(a)=1,\text{level}(f)=2,\text{level}(j)=3.$$

进一步,该树的深度为 3.

有根树 T 给了边的方向这个事实是指能够给出点与点之间的优先关系.特别地,称顶点 u 优先顶点 v 或 v 跟随 u,如果存在一条从 u 到 v 的有向路,特别,若(u,v)为一条边,即 v 跟随 u,且 v 从 u 邻接,则称 v 紧跟 u.注意到除了根外的每个顶点紧跟一个惟一的顶点,但 v 可以被多于一个顶点紧跟.例如,在图 9-3 中,顶点 j 跟随 c,但紧跟 g,也有,i 和 j 紧跟 g.

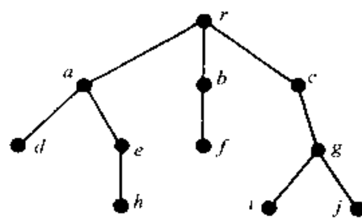


图 9-3

当每个事件发生的方式有限时,有根树在枚举一系列事件的所有逻辑可能时是非常有用的工具,这用下面的例子说明.

例 9.5　设 Marc 和 Erik 正进行网球比赛,规定先连赢两场或赢得三场者获胜,求比赛可能进行的方法数.

图 9-4 中的有根树(根在左边)给出了比赛能进行的各种方式.有 10 个树叶,对应着比赛可能发生的 10 种方法:

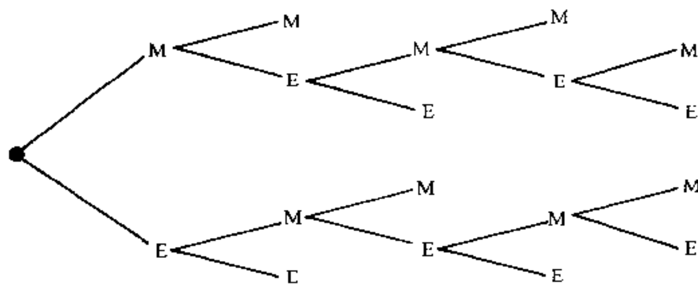


图 9-4

MM,MEMM,MEMEM,MEMEE,MEE,EMM,EMEMM,EMEME,EMEE,EE.

特别地,从根到树叶的路描述了在特定的比赛中谁会赢得哪一场比赛.

有序根树

考虑有根树 T,其中离开每个顶点的边有序.于是有*有序根树*的概念,可以如下系统地标号(指定地址)这样的树的顶点:给根 r 标号 0,接着根据边的次序,用 1,2,3,…,标号紧跟 r 的顶点,然后按下面的方法标号剩下的顶点,若 a 为顶点 v 的标号,则用 $a.1$,$a.2$,…按照边的次序给紧跟 v 的顶点标号.图 9-5 解释了这种标号系统,这里根据边的次序边从左到右画出边.注意到标号中小数点的数目小于顶点的层次,对有序根树,称这样的标号系统为*通用地址系统*.

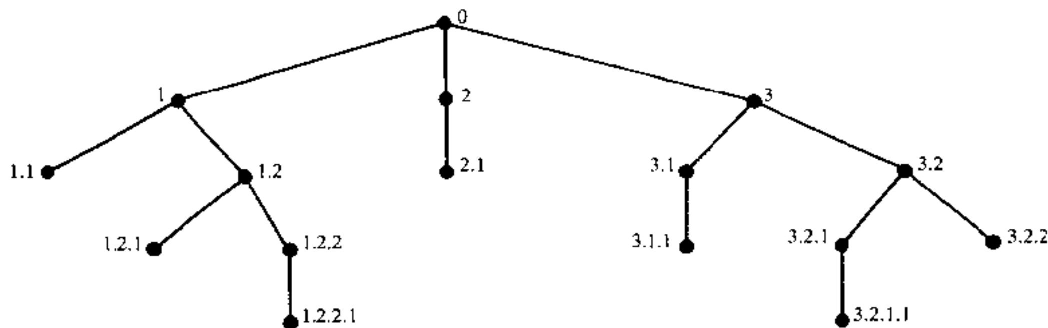


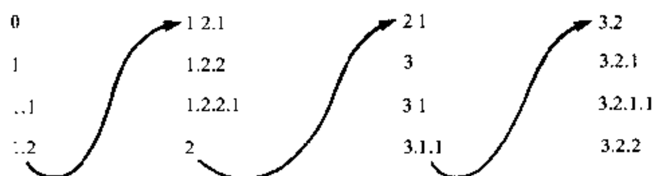
图 9-5

通用地址系统给出了描述(或存贮)有序根树的一个重要方法.特别地,已知地址 a 和 b,若 a 为 b 的*初始节*,即若 $b=a.c$ 或者,若存在正整数 m 和 n,$m<n$ 使得

$$a=r.m.s \text{ 和 } b=r.n.t.$$

则记 $a<b$.这个次序称为*字典序*,因为它类似于字典里单词的排列.例如,图 7-5 中的地址被

如下线性排序.



该字典序与沿树的最左分支向右移,再沿紧邻的右边的分支向右移,再沿右边的第二个分支,等等所得到的序是一致的.

代数式与波兰记号

任何涉及二元运算,例如加、减、乘、除的代数式都可用一棵有序根树来表示. 例如,图9-6(a)表示算式

$$(a-b)/((c\times d)+e) \tag{9.1}$$

注意到式中的变量 a,b,c,d,e 作为树叶出现,而运算作为其他顶点出现,树必须是有序的,因为 $a-b$ 和 $b-a$ 给出相同的树,但不给出相同的有序根树.

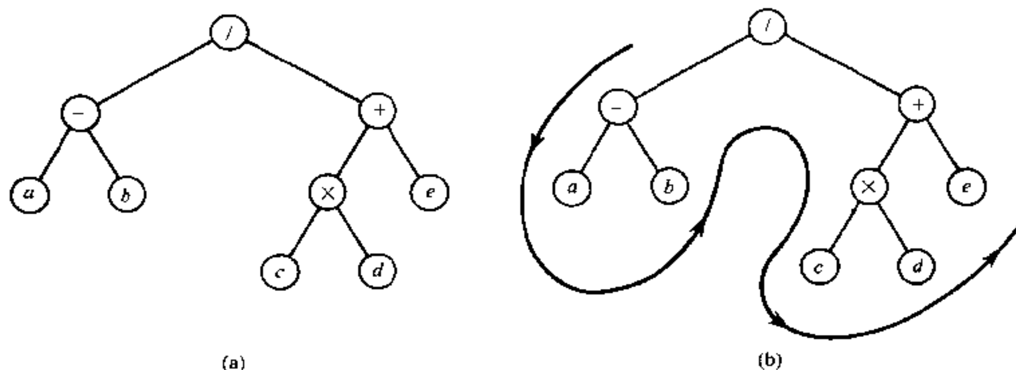


图 9-6

波兰数学家 Lukasiewicz 注意到若将二元运算符号放在运算对象之前,例如,

$$+ab \text{ 代替 } a+b, /cd \text{ 代替 } c/d,$$

则,人们就不必使用任何括号,这个记号称为*前缀形式波兰记号*(相应地,可以将符号放在对象的后面,称为*后缀形式波兰记号*). 用前缀形式波兰记号重写(9.1)式得到

$$/-ab+\times cde$$

注意到这恰好是扫描图 9-6(b)中的树得到的该树顶点字典序.

9.5　有向图的序列表示

在计算机中存贮有向图 G 有两个主要方法. 一种方法,称为 G 的*序列表示*,是用它的邻接矩阵 A 表示. 另一种方法,称为 G 的*链表示*,是用邻点的链表表示. 本节讨论第一种表示,并说明如何地应用 G 的邻接矩阵 A,来方便地回答 G 的连通度的某些问题. 链表示将在§9.7讨论.

设图 G 有 m 个顶点和 n 条边,若 $m=O(n^2)$,则称 G 为*稠密的*,若 $m=O(n)$,或 $m=O(n\log n)$,则称 G 为*稀疏的*,当 G 稠密时,G 常用矩阵表示,而当 G 稀疏时,常用链表示. 无论用哪种方法存贮 G,图 G 通常都以它的正式定义,即以顶点集和边集(点对集)形式存贮于计算机中.

注　为避免特例情况,除非特别指明,总假设 $m>1$,m 为图 G 的顶点数. 因此,若 G 没有边,则 G 不可能连通.

有向图与关系,邻接矩阵

设$G(V,E)$为简单有向图,即没有平行边的图,则E简化为$V\times V$的子集,因此,E为V上的一个关系.反过来,若R为V上的一个关系,则$G(V,R)$为一个简单有向图.于是,集合上的关系的概念就与简单有向图是同一个概念,事实上,在第二章,对应于集合上的关系就已引入有向图.

设G为m个顶点的简单有向图,且设G的顶点被排序,称为$v_1,v_2,\cdots,v_m$.则G的邻接矩阵$A=[a_{ij}]$是如下定义的$m\times m$矩阵.

$$a_{ij}=\begin{cases}1,\text{若存在边}(v_i,v_j),\\0,\text{否则}.\end{cases}$$

这样的只含0,1的矩阵称为比特矩阵或布尔矩阵.

图G的邻接矩阵A依赖于G的顶点的次序.即不同的顶点序可能产生不同的邻接矩阵.不过,两个不同次序得到矩阵密切相关,只要简单地互换行和列就可从一个矩阵得到另一个矩阵.除非指明,总设讨论的矩阵有一个固定的顶点次序.

注1 邻接矩阵$A=[a_{ij}]$也可推广到有平行边的有向图,令

$$a_{ij}=\text{始于 }v_i,\text{终于 }v_j\text{ 的边的条数},$$

则A的每个元素为非负整数.反过来,每个非负整数的$m\times m$矩阵惟一地定义了一个m个顶点的有向图.

注2 若G为无向图,则G的邻接矩阵A为对称矩阵,即对每个i和j有$a_{ij}=a_{ji}$.这是由于每条无向边$\{u,v\}$对应了两条有向边(u,v)和(v,u).

例9.6 考虑图9-7中的有向图G,其顶点为X,Y,Z,W.设顶点如下排序:

$$v_1=X,\ v_2=Y,\ v_3=Z,\ v_4=W.$$

则G的邻接矩阵A为

$$A=\begin{bmatrix}0&0&0&1\\1&0&1&1\\1&0&0&1\\1&0&1&0\end{bmatrix}.$$

注意到A中1的个数等于边的条数(8).

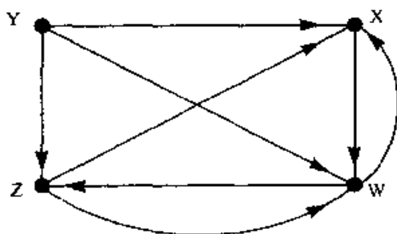


图9-7

考虑图G的邻接矩阵$A=[a_{ij}]$的幂$A,A^2,A^3,\cdots$.采用下面的记号:

$$a_k(i,j)=\text{矩阵 }A^k\text{ 中第 }i\text{ 行第 }j\text{ 列的元素}.$$

由于$a_1(i,j)=a_{ij}$为从顶点v_i到v_j的长为1的路的条数,因而可以证明$a_2(i,j)$为从v_i到v_j的长为2的路的条数.事实上,在问题9.14中,我们将证明下面的一般结果.

命题9.4 设A为图G的邻接矩阵,则矩阵A^k的第i行第j列的元素$a_k(i,j)$给出了从v_i到v_j的长为k的路的条数.

例9.7 再考虑图9-7中的图G,其邻接矩阵A如例9.6,A的幂A^2,A^3,A^4如下:

$$A^2=\begin{bmatrix}1&0&1&0\\2&0&1&2\\1&0&1&1\\1&0&0&2\end{bmatrix},A^3=\begin{bmatrix}1&0&0&2\\3&0&2&3\\2&0&1&2\\2&0&2&1\end{bmatrix},A^4=\begin{bmatrix}2&0&2&1\\5&0&3&5\\3&0&2&3\\3&0&1&4\end{bmatrix}.$$

注意到 $a_2(4,1)=1$，故从 v_4 到 v_1 有一条长为 2 的路，又 $a_3(2,3)=2$，故从 v_2 到 v_3 有 2 条长为 3 的路. 而 $a_4(2,4)=5$，故从 v_2 到 v_4 有 5 条长为 4 的路.（这里 $v_1=X,v_2=Y,v_3=Z,v_4=W$）.

注 设 A 为图 G 的邻接矩阵，且如下定义矩阵 B_r.

$$B_r=A+A^2+A^3+\cdots+A^r.$$

则矩阵 B_r 的第 i 行第 j 列的元素给出了从顶点 v_i 到 v_j 的长至多为 r 的路的条数.

路矩阵

设 $G=G(V,E)$ 为有 m 个顶点 $v_1,v_2,\cdots,v_m$ 的简单有向图. G 的**路矩阵**，或**可达矩阵**为 m 阶方阵 $P=(p_{ij})$，其中

$$p_{ij}=\begin{cases}1,\text{若有从 } v_i \text{ 到 } v_j \text{ 的路},\\0,\text{否则}.\end{cases}$$

（下一小节给出路矩阵 P 可看作 V 上关系 E 的传递闭包.）

设 m 个顶点的图 G 中有一条从 v_i 到 v_j 的路，则当 $v_i\neq v_j$ 时，必有一条从 v_i 到 v_j 的简单路；或当 $v_i=v_j$ 时，必有一条从 v_i 到 v_j 的圈. 由于 G 有 m 个顶点，所以这样的简单路的长至多为 $m-1$，或这样的圈的长至多为 m. 这就是说，矩阵

$$B_m=A+A^2+A^3+\cdots+A^m$$

第 i 行第 j 列的元素非 0，这里 A 为 G 的邻接矩阵. 因此，路矩阵 P 与 B_m 有相同的非 0 元素. 正式叙述这个结果：

命题 9.5 设 A 为 m 个顶点的图 G 的邻接矩阵. 且设

$$B_m=A+A^2+A^3+\cdots+A^m.$$

则路矩阵 P 与 B_m 有相同的非零值.

回忆对有向图 G 的任一对顶点 u 和 v，如果存在从 u 到 v 以及从 v 到 u 的路，则 G 称为强连通的，因此，G 为强连通的当且仅当 G 的路矩阵 P 没有零值. 由这个事实与命题 9.5 得到下面的结果：

命题 9.6 设 A 为 m 个顶点的图 G 的邻接矩阵. 且设

$$B_m=A+A^2+A^3+\cdots+A^m.$$

则 G 是强连通的当且仅当 B_m 没有零值.

例 9.8 考虑图 9－7 中 $m=4$ 个顶点的图 G，这里设 $v_1=X,v_2=Y,v_3=Z,v_4=W$. 相加例 9.6 和例 9.7 中的矩阵 A,A^2,A^3 和 A^4，得到下面的矩阵 B_4. 用 1 取代 B_4 中的非零值，便得到图 G 的路(可达)矩阵 P：

$$B_4=\begin{bmatrix}4&0&3&4\\11&0&7&11\\7&0&4&7\\7&0&4&7\end{bmatrix},P=\begin{bmatrix}1&0&1&1\\1&0&1&1\\1&0&1&1\\1&0&1&1\end{bmatrix}.$$

检查矩阵 B_4 或 P，发现有零值，因此 G 不是强连通的. 特别地，可以看出从任何其他顶点都不可到达顶点 $v_2=Y$.

注 图 G 的邻接矩阵 A 和路矩阵 P 可看成逻辑(布尔)矩阵. 其中 0 表示“假”，1 表示“真”，于是逻辑运算 $\wedge$(与)和 $\vee$(或)，其值见图 9－8，可应用到 A 和 P 的值，下节将使用这些运算.

∧	0	1
0	0	0
1	0	1

(a) 与

∨	0	1
0	0	1
1	1	1

(b) 或

图 9－8

传递闭包与路矩阵

设 R 为 m 个元素的有限集 V 上的关系. 如上所述，关系 R 可看成简单有向图 $G=G(V,R)$，回忆(2.5 节)定义的合成关系 $R^2=R\circ R$，$R^2=\{(u,v):$存在 $w\in V$，使得$(u,w)\in R$，且$(w,v)\in R\}$. 换句话说，R^2 由所有的存在从 u 到 v 的长为 2 的路的点对(u,v)组成. 类似地，

$R^k=\{(u,v):$存在从 u 到 v 的长为 k 的路$\}$.

V 上关系 R 的传递闭包 R^* 可看成是有序对(u,v)的集合，使得 G 中存在从 u 到 v 的路. 因此，$G=G(V,R)$的路矩阵 P 恰好是图 $G'=G'(V,R^*)$的邻接矩阵. 图 G' 对应于传递闭包 R^*. 进一步，由上面的讨论. 我们只需查看长至多为 $m-1$ 的简单路与长至多为 m 的圈，因而有下面的结论，它刻画了 R 的传递闭包 R^*.

定理 9.7　设 R 为 m 个元素的集合 V 上的一个关系，则

(i) $R^*=R\cup R^2\cup\cdots\cup R^m$ 为 R 的传递闭包.

(ii) $G(V,R)$的路矩阵 P 为 $G'(V,R^*)$的邻接矩阵.

9.6　Warshall 算法，最短路

设 G 为 m 个顶点的有向图，其 m 个顶点为 $v_1,v_2,\cdots,v_m$，假定要求图 G 的路矩阵 P. Warshall 给了一个算法，该算法比计算邻接矩阵 A 的幂更有效. 本节讨论这样的算法. 当 G 为赋权图时，类似的算法用于求赋 G 的最短路.

Warshall 算法

首先如下定义 m 阶布尔矩阵 $P_0,P_1,\cdots,P_m$，设 $P_k[i,j]$表示矩阵 P_k 的第 i 行第 j 列的元素. 定义：

$$P_k[i,j]=\begin{cases}1,\text{若存在从 } v_i \text{ 到 } v_j \text{ 的简单路，且这条路上除了 } v_1,v_2,\cdots,v_k \text{ 外没有其他顶点,}\\0,\text{否则.}\end{cases}$$

即

$P_0[i,j]=1$　　若存在从 v_i 到 v_j 的边.

$P_1[i,j]=1$　　若存在从 v_i 到 v_j 的简单路，这条路上除了可能有 v_1 外没有其余顶点.

$P_2[i,j]=1$　　若存在从 v_i 到 v_j 的简单路，这条路上除了可能有 v_1 和 v_2 外没有其他顶点. 等等.

注意到第一个矩阵即为 G 的邻接矩阵 $P_0=A$. 进一步，由于 G 仅有 m 个顶点，所以最后一个矩阵 P_m 就是 G 的路矩阵 P，即 $P_m=P$.

Warshall 注意到仅当下列两情形之一发生时，$P_k[i,j]=1$.

(1) 存在从 v_i 到 v_j 的简单路，这条路除了可能有 $v_1,v_2,\cdots,v_{k-1}$ 外没有其他顶点. 因此，

$$P_{k-1}[i,j]=1.$$

(2) 存在从 v_i 到 v_k 的简单路和从 v_k 到 v_j 的简单路，且每条简单路除了可能有 $v_1,v_2,\cdots,v_{k-1}$ 外没有其他顶点. 因此，

$$P_{k-1}[i,k]=1,\text{且 } P_{k-1}[k,j]=1.$$

这两种情形如下表示

$$(1)\ v_i \to \cdots \to v_j;\ (2)\ v_i \to \cdots \to v_k \to \cdots \to v_j.$$

而

$$\to\cdots\to$$

表示简单路的部分,该简单路除了可能有 $v_1, v_2, \cdots, v_{k-1}$ 外没有其他顶点. 因此,P_k 的元素由

$$P_k[i,j] = P_{k-1}[i,j] \vee (P_{k-1}[i,k] \wedge P_{k-1}[k,j])$$

得到. 这里使用了逻辑运算 ∧(与)和 ∨(或). 换句话说,只要看矩阵 P_{k-1} 中的三个值就可得到 P_k 中的一个值. Warshall 算法如下:

算法 9.6(Warshall 算法) M 个顶点的有向图 G 用其邻接矩阵 A 存贮,该算法求图 G 的(布尔)路矩阵 P.

Step 1 对 $I, J = 1, 2, \cdots, M$ 重复:(初始化 P.)
　　若 $A[I,J]=0$,则置 $P[I,J]:=0$;
　　否则,置 $P[I,J]:=1$.
　[结束循环.]

Step 2 对 $K=1,2,\cdots,M$,重复 Step 3 和 Step 4:(刷新 P)

Step 3 对 $I=1,2,\cdots,M$ 重复 Step 4:

Step 4 对 $J=1,2,\cdots,M$ 重复:
　置 $P[I,J]:=P[I,J] \vee (P[I,K] \vee P[K,J])$.
　[结束循环.]
　[结束 Step 3 循环.]
　[结束 Step 2 循环.]

Step 5 退出.

最短路算法

设 G 为 m 个顶点的有向图,其 m 个顶点为 $v_1, v_2, \cdots, v_m$. 且设 G 为赋权的,即 G 的每条边指派一个非负数 $w(e)$,称为 e 的**权**或**长度**. 则 G 可用它的权矩阵存贮,其中**权矩阵** $W=(w_{ij})$ 如下定义:

$$w_{ij} = \begin{cases} w(e), & \text{若有从 } v_i \text{ 到 } v_j \text{ 的边 } e, \\ 0, & \text{若没有从 } v_i \text{ 到 } v_j \text{ 的边.} \end{cases}$$

路矩阵 P 揭示了任两点之间是否存在路,现要求一个矩阵 Q,使得 Q 揭示了任两点之间的最短路的长度,或更确切地说,求一个矩阵 $Q=(q_{ij})$. 其中

$$q_{ij} = \text{从 } v_i \text{ 到 } v_j \text{ 的最短路的长度}.$$

下面我们给出修改的 Warshall 算法,它能有效地求出矩阵 Q.

定义矩阵序列 $Q_0, Q_1, \cdots, Q_m$(类似于上面的矩阵 $P_0, P_1, \cdots, P_m$),其中 Q_k 的第 i 行第 j 列的元素 $Q_k[i,j]$ 如下定义:

$Q_k[i,j]$= 前面从 v_i 到 v_j 的路长与前面从 v_i 到 v_k 以及从 v_k 到 v_j 的路长之和的较小者. 更确切地,

$$Q_k[i,j] = \text{MIN}(Q_{k-1}[i,j], Q_{k-1}[i,k] + Q_{k-1}[k,j])$$

初始矩阵 Q_0,除了 W 中的每个 0 换为∞(或一个非常非常大的数)外,恰好就是权矩阵 W,最后的矩阵 Q_m 就为所需矩阵 Q.

例 9.9 图 9-9 给了一赋权图 G 以及它的权矩阵 W,这里 $v_1=R, v_2=S, v_3=T, v_4=U$.

假设对赋权图 G 用修改的 Warshall 算法,便得到图 9-10 中的矩阵 Q_0, Q_1, Q_2, Q_3 和 Q_4. (在图 9-10 中每个矩阵 Q_k 的右边,给出了对应于矩阵 Q_k 的长度的路的矩阵.)矩阵 Q_0 与权矩阵 W 有相同的值,只是 W 中的每个 0 换为∞(或一个很大的数). 这里指明带圆圈的值是如

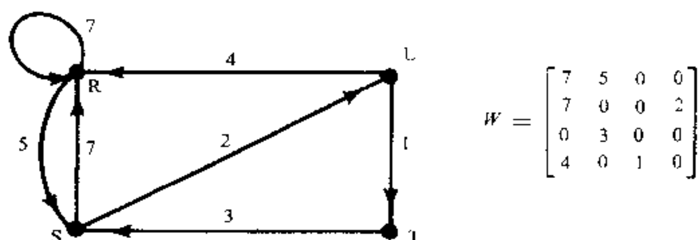


图 9－9

何得到的：

$$Q_1[4,2]=\mathrm{MIN}(Q_0[4,2],Q_0[4,1]+Q_0[1,2])=\mathrm{MIN}(\infty,4+5)=9,$$
$$Q_2[1,3]=\mathrm{MIN}(Q_1[1,3],Q_1[1,2]+Q_1[2,3])=\mathrm{MIN}(\infty,5+\infty)=\infty,$$
$$Q_3[4,2]=\mathrm{MIN}(Q_2[4,2],Q_2[4,3]+Q_2[3,2])=\mathrm{MIN}(9,3+1)=4,$$
$$Q_4[3,1]=\mathrm{MIN}(Q_3[3,1],Q_3[3,4]+Q_3[4,1])=\mathrm{MIN}(10,5+4)=9.$$

最后的矩阵 $Q_4=Q$，即为所求的最短路矩阵.

$$Q_0=\begin{bmatrix}7&5&\infty&\infty\\7&\infty&\infty&2\\\infty&3&\infty&\infty\\4&\infty&1&\infty\end{bmatrix},\begin{bmatrix}RR&RS&—&—\\SR&—&—&SU\\—&TS&—&—\\UR&—&UT&—\end{bmatrix},$$

$$Q_1=\begin{bmatrix}7&5&\infty&\infty\\7&12&\infty&2\\\infty&3&\infty&\infty\\4&\textcircled{9}&1&\infty\end{bmatrix},\begin{bmatrix}RR&RS&&—\\SR&SRS&—&SU\\—&TS&—&—\\UR&URS&UT&—\end{bmatrix},$$

$$Q_2=\begin{bmatrix}7&5&\textcircled{\infty}&7\\7&12&\infty&2\\10&3&\infty&5\\4&9&1&11\end{bmatrix},\begin{bmatrix}RR&RS&—&RSU\\SR&SRS&—&SU\\TSR&TS&—&TSU\\UR&URS&UT&URS\end{bmatrix},$$

$$Q_3=\begin{bmatrix}7&5&\infty&7\\7&12&\infty&2\\10&3&\infty&5\\4&\textcircled{4}&1&6\end{bmatrix},\begin{bmatrix}RR&RS&—&RSU\\SR&SRS&—&SU\\TSR&TS&—&TSU\\UR&UTS&UT&UTSU\end{bmatrix},$$

$$Q_4=\begin{bmatrix}7&5&8&7\\7&11&3&2\\\textcircled{9}&3&6&5\\4&4&1&6\end{bmatrix},\begin{bmatrix}RR&RS&RSUT&RSU\\SR&SURS&SUT&SU\\TSUR&TS&TSUT&TSU\\UR&UTS&UT&UTSU\end{bmatrix}.$$

图 9－10

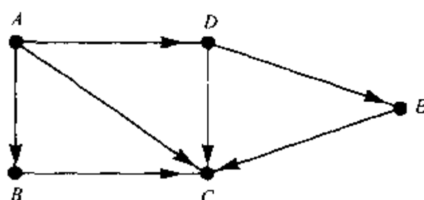
9.7 有向图的链表示

设 G 为 m 个顶点的有向图. 并设 G 的边数是 $O(m)$ 或甚至为 $O(m\log m)$. 即假设 G 为稀疏的，则 G 的邻接矩阵 A 含有许多 0. 因而大量的存贮空间被浪费了. 因此，当 G 稀疏时，G 通常用某种链表示存贮，这种链表示称为邻接结构. 下面用例子说明.

考虑图 9－11(a)中的有向图 G，注意到 G 也可以用图 9－11(b)中表等价地定义. 该表给出了 G 中的每个顶点以及紧跟的邻接表，称为其后继或邻点. 而符号 $\varnothing$ 表示空表. 又 G 的每条边也对应着邻接表中的惟一顶点，反之亦然. 该图 G 有 7 条边因而邻接表中有 7 个顶点，该表可用紧凑格式给出：

$$G=[A:B,C,D;B:C;C:\varnothing;D:C,E;E:C]$$

这里冒号“:”分隔了顶点及其邻点表,而分号“;”分隔了不同的表.



(a) 图 G

顶点	邻接表
A	B, C, D
B	C
C	$\varnothing$
D	C, E
E	C

(b) G的邻接表

图 9-11

有向图 G 的链表示用其邻接表的链表存贮 G. 特别地,链表示通常含有两个文件(记录的集合),一个称为点文件,另一个称为边文件. 如下所示:

(a) 点文件 图 G 通常用一数组或一链表存贮,点文件包含图 G 的顶点列表,点文件的每个记录有如下形式

VERTEX	NEXT-V	PTR	

这里 VERTEX 为顶点名,NEXT-V 指向点文件中顶点列表的下一顶点,而 PTR 指向边文件中顶点的邻接表的第一个元素,阴影区域说明对应于该点的记录中也许还有其他信息.

(b) 边文件 边文件含有 G 的边以及 G 的全部邻接表,而每个邻接表用链表存贮. 边文件的每个记录将表示 G 的惟一边,因而对应于邻接列表的惟一顶点,该记录有如下形式:

EDGE	BEG-V	END-V	NEXT-E	

这里:

(1) EDGE 为边名(若有边名的话).

(2) BEG - V 指出该边的起点顶点文件中的地址.

(3) END - V 指出该边的终点顶点文件中的地址. 邻接表就在该字段内.

(4) NEXT-E 指出邻接表的下一顶点边文件中的地址.

需强调的是,邻接表由终点构成,因而用 END-V 字段存贮. 阴影部分说明对应于该边的记录也许有其他信息. 注意邻接列表中顶点的次序依赖于边(点对)在输入中出现的次序.

图 9-12 显示如何存贮图 9-11(a)中的图 G,这里 G 的顶点用指向第一个顶点的变量 START 的链表存贮.(此外,也可用顶点列表的线性组,此时 NEXT-V 将不需要.)点文件的 8 个地址与边文件的 10 个地址是任意的. 若在图中插入额外的顶点或边就用文件中的额外位

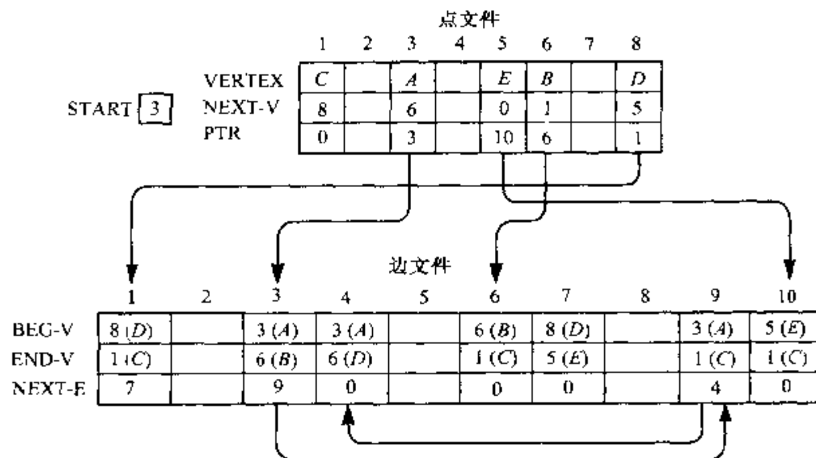


图 9-12

置. 图 9－12 也用箭头给出顶点 A 的邻接表$[B,C,D]$.

9.8　图算法:深度优先查找与广度优先查找

本节对给定图 G 讨论两个重要的图算法. 任何特定的图算法都可能依赖于 G 的存贮方式. 这里假定 G 用邻接结构存贮. 图 9－13 给出了测试图 G 的邻接结构.

图的许多应用要求人们系统地检查图 G 的顶点与边. 有两种标准的方法来实现，一种方法称为**深度优先查找**(DFS)，另一种称为**广度优先查找**(BFS).(这些算法本质上与第八章无向图的相应算法一致.)

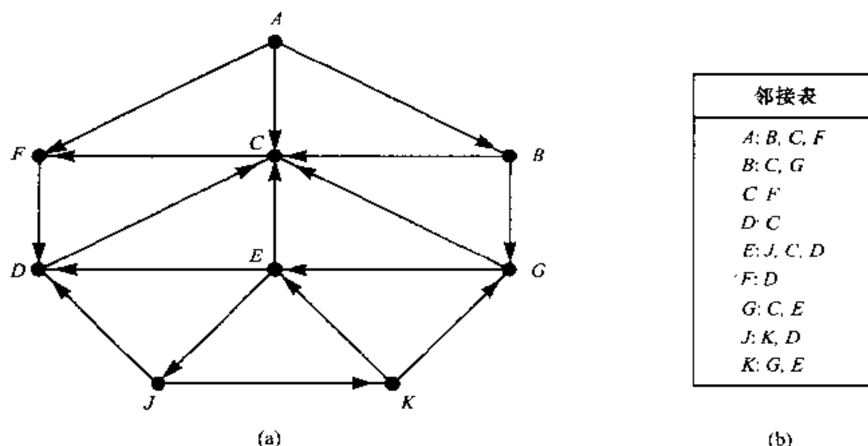


图 9－13

在执行算法时，G 的每个顶点 N 处于如下三种状态之一，称为 N 的状态：

STATUS＝1：　(准备状态)　顶点 N 的初始状态.

STATUS＝2：　(等候状态)　顶点 N 在等候表中，等候进行.

STATUS＝3：　(检查状态)　顶点 N 已经检查.

深度优先查找的等候列表是一个(修改的)堆栈，而广度优先查找的等候列表是 QUEUE(队列).

(a) **深度优先查找**:从 A 开始的深度优先查找的主要思想如下. 首先检查开始点 A，然后沿以 A 开头的路 P 检查每一个顶点 N；即进行 A 的邻点，再检查 A 的邻点的邻点，等等. 在到达"死点"后，即到达一个没有可检查的邻点的点后，沿路 P 反向追踪，直到可以沿另一条路 P' 继续下去，等等. 反向追踪用堆栈实现，它包含了将来可能的路的起点. 我们还需要字段 STATUS 来告诉我们所有顶点当前的状态，使得没有顶点被检查超过一次. 算法如下：

算法 9.8A(深度优先查找)　设 G 为有向图，该算法执行了从 A 点开始的深度优先查找.

Step 1　初始化全部点到准备状态(STATUS＝1).

Step 2　将开始点 A 放到堆栈上，并改变 A 的状态为等候状态(STATUS＝2).

Step 3　重复 Step 4 和 Step 5，直到堆栈空.

Step 4　移去 STACK 的顶点 N，检查 N，并置 STATUS(N)＝3，检查状态.

Step 5　检查 N 的每个邻点 J.

(a) 若 STATUS(J)＝1(准备状态)，将 J 放到堆栈上，并重置STATUS(J)＝2(等候状态).

(b) 若 STATUS(J)＝2(等候状态)，从堆栈中删去前一个 J，且将当前的 J 放到堆栈上.

(c) 若 STATUS(J)＝3(检查状态)，跳过顶点 J.

[结束 Step 3 循环.]

Step 6　退出.

上面算法仅检查从开始点 A 可到达的那些顶点. 假定要检查图 G 的所有顶点，那么应修

改算法，使得它再从一个仍处于准备状态(STATUS=1)的点开始. 这个新的顶点，设为 B，可通过走遍顶点列表得到.

注　上述算法中结构堆栈技术上并不是一个堆栈. 因为，在 Step 5(b)，允许删除顶点 J，然后在堆栈的前面插进 J.(尽管是同一个顶点 J，但它表示不同的边.)如果在 Step 5(b)不将 J 移到堆栈的顶. 那么就得到另一个横截算法.

例 9.10　考虑图 9-13 的测试图 G. 假设要求并打印由顶点 J 可到达的所有顶点(包括 J 本身). 实现它的一种方法是利用开始于 J 的 G 的深度优先查找.

应用算法 9.8A，顶点按如下次序检查，并打印：

$$J,\ K,\ G,\ E,\ C,\ F,\ D.$$

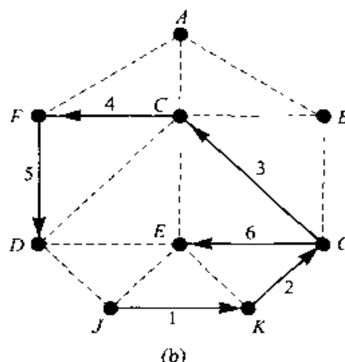
特别地，图 9-14(a)给出堆栈中等候列表序列以及正被进行的顶点(斜杠/指出顶点从等候列表中删除.)强调一下，每个顶点(包括 J)取自邻接列表，因而它是该图的惟一一条边的终点. 且通过预先标号具有该边起点的终点来指定边. 例如，

$$J^D$$

指 D 在 J 的邻接表中，因而 D 为起于 J 的某边的终点. 这些边构成了以 J 为根的有根树，见图 9-14(b).(这些数指出被加到树 T 上边的次序). 这棵树 T 支撑着 G 的子图 G'，G' 由从 J 可到达的顶点构成.

顶点	堆栈
	J
J	J^K, J^D
J^K	K^G, K^E, J^D
K^G	G^C, G^E, K^E, K^D
G^C	C^F, G^E, K^D
C^F	F^D, G^E, K^D
F^D	G^E
G^E	$\varnothing$

(a)



(b)

图 9-14

(b) **广度优先查找**　开始于顶点 A 的广度优先查找的主要思想如下. 首先检查起点 A，然后检查 A 的所有邻点，再检查 A 的邻点的所有邻点，等等. 自然地，需要保留一个顶点的邻点的轨迹，还要保证没有点被检查两次. 利用队列包含等候检查的顶点，用字段 STATUS 记取顶点的当前状态. 由此，利用队列和 STATUS 就可实现，算法如下.

算法 9.8B(广度优先查找)　该算法对有向图 G 执行开始于 A 点的广度优先查找.

Step 1　初始化所有顶点到准备状态(STATUS=1).

Step 2　将 A 放进队列，且将 A 的状态改为等候状态(STATUS=2).

Step 3　重复 Step 4 与 Step 5，直到队列空.

Step 4　移去队列的第一点 N，检查 N，并置 STATUS(N)=3，检查状态.

Step 5　检查 N 的每个顶点 J.

(a) 若 STATUS(J)=1(准备状态)，则将 J 加到队列的后面，重置 STATUS(J)=2(等候状态).

(b) 若 STATUS(J)=2(等候状态)或 STATUS(J)=3(检查状态)，跳过 J.

[结束 Step 3 循环.]

Step 6　退出.

同样，上面算法仅检查从起点 A 可到达的那些顶点. 若要检查图 G 的所有顶点，则该算法必须修改，使得它再开始于仍处于准备状态(STATUS=1)的另一个顶点. 这个新的顶点，记

作 B,可通过走遍顶点列表得到.

例 9.11　考虑图 9-13 中的图 G. 假设 G 表示城市间的每日航班. 若要从城市 A 飞到城市 J,使得逗留的城市数最少,即找一条从 A 到 J 的最短路 P(此时,每条边的权为 1). 则一种方法就是对图 G 用开始于 A 点的广度优先查找,一旦碰到 J,即一旦 J 加到等候列表,就停止.

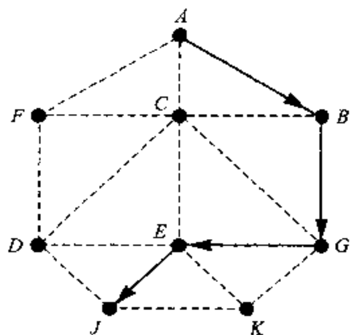
图 9-15(a)给出了队列中等候列表的序列以及碰到 J 时已进行的顶点,那么从 J 反向追踪就得到所需的路.

$$E^J \leftarrow G^E \leftarrow B^G \leftarrow A^B \leftarrow A \text{ 或 } A \rightarrow B \rightarrow G \rightarrow E \rightarrow J.$$

见图 9-15(b),这样,从城市 A 飞到城市 J 的航班有三个中间逗留,B,G 和 E. 注意到这条路并未包含算法检查的所有顶点.

顶点	队列
	A
A	A^B, A^C, A^F
A^F	F^D, A^B, A^C
A^C	F^D, A^B
A^B	B^G, F^D
F^D	B^G
B^G	G^E
G^E	E^J

(a)



(b)

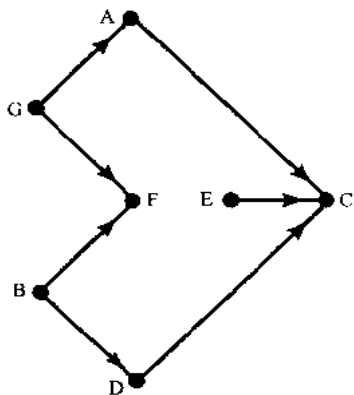
图 9-15

9.9　有向无圈图,拓扑排序

设 S 为有向图,使得(1) S 的每个顶点 v_i 表示一件任务,(2) S 的每条(有向边)(u,v)表示在任务开始 v 之前,任务 u 必须完成. 假设这样一个图 S 含有圈,比如

$$P=(u,v,w,u),$$

意味着 v 开始之前必须完成 u,开始 w 之前必须完成 v,而 u 开始之前必须完成 w. 因而,不能开始圈中三个任务中的任何任务. 于是,表示任务及先决条件的这样一个图 S 不能有任何圈. 换句话说,这样的图 S 必为无圈的. 有向无圈图简称为 dag(directed acyclic graph 的三个第一个字母). 图9-16就是这样的一个例子.



(a)

邻接表	
A:	C
B:	D, F
C:	
D:	C
E:	C
F:	
G:	A, F

(b)

图 9-16

dag S 上的基本运算就是一个接一个地检查顶点,使得当(u,v)是一条边时,顶点 u 总在顶点 v 之前检查. S 的顶点的线性序 T 称为拓扑排序,也许不惟一. 图 9-17 给出了图 9-16

中图 S 的两个拓扑排序. 为说明 S 的边与线性序的方向一致,图 9 - 17 中包含了 S 的所有边.

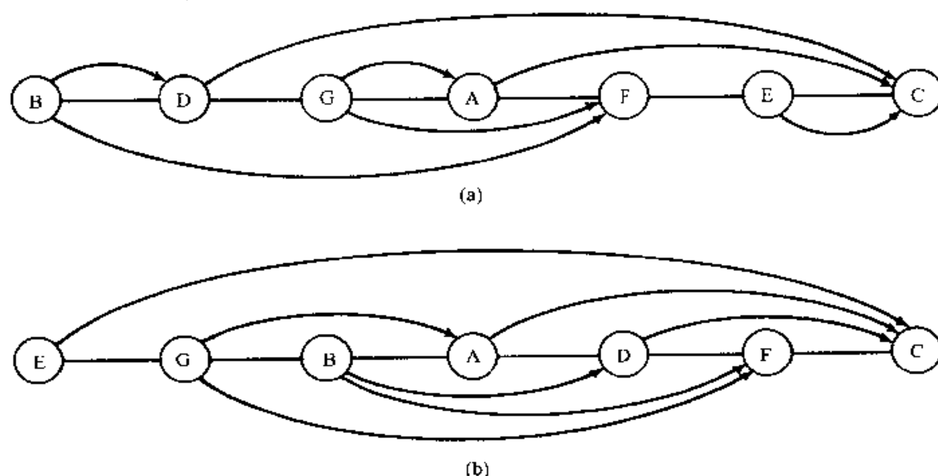


图 9 - 17 两个拓扑排序

下面是本节的主要理论结果.

定理 9.8 设 S 为有限的有向无圈图. 则图 S 存在一个拓扑排序 T.

注意到定理仅陈述拓扑排序存在. 现给出求拓扑排序的一个算法. 该算法的主要思想是零入度的任何顶点 N 可选为排序 T 的第一个元素. 该算法本质上重复下面的两步,直到 S 为空:

(1) 找零入度的顶点 N.

(2) 从图 S 中删去 N 及它的边.

用辅助队列暂存所有零度顶点,算法如下:

算法 9.9 求有向无圈图 S 的拓扑排序的算法.

Step 1 求 S 的每个顶点 N 的入度 INDEG(N).

Step 2 在队列中插入所有的零度顶点.

Step 3 重复 Step 4 和 Step 5,直到队列空.

Step 4 移去并检查队列的前面顶点 N.

Step 5 对顶点 N 的每个邻点 M 重复.

(a) 置 INDEG(M) := INDEG(M) − 1.

[删除从 N 到 M 的边.]

(b) 若 INDEG(M) = 0,则添加 M 到队列.

[结束循环.]

[结束 Step 3 循环.]

Step 6 退出.

例 9.12 设对图 9 - 16 中的图 S 应用算法 9.9,则得到队列中元素的序列以及被检查的顶点序列,如下表.

顶点		B	E	G	D	A	F	C
队列	GEB	DGE	DG	FAD	FA	CF	C	$\varnothing$

图 9 - 18 给出了从 S 中删去前三个顶点的每一个及其边的那个图 S,拓扑排序 T 就是检查顶点的序列,即

$$T: B, E, G, D, A, F, C.$$

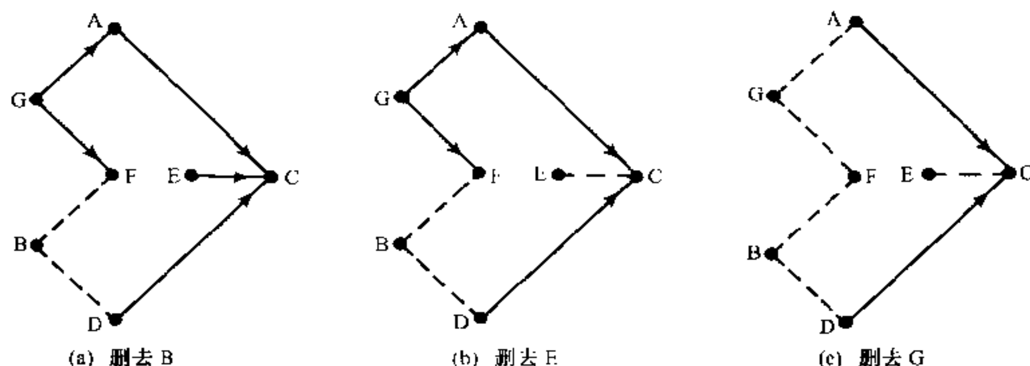


图 9-18

9.10 最短路的修剪算法

设 G 为赋权有向无圈图，寻求 u 和 w 两点之间的最短路. 假设 G 是有限的，因此每一步有有限次移动. 由于 G 是无圈的，所以 u 和 w 之间的所有路可由以 u 为根的有根树给出，图 9-19(b)列举了图 9-19(a)中点 u 与 w 之间的所有路.

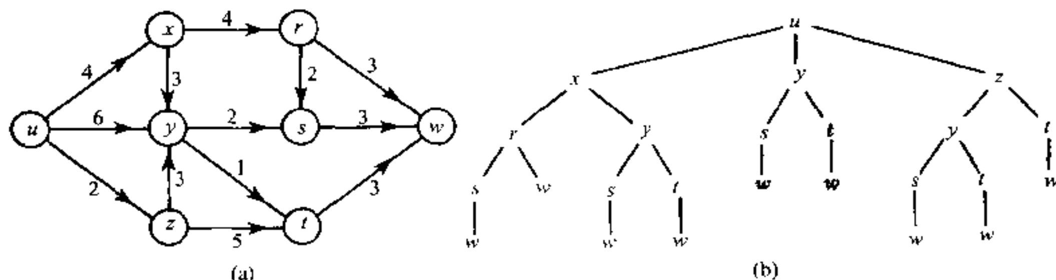


图 9-19

求 u 与 w 之间的最短路的一种方法就是简单计算相应有根树中所有路的长度. 另一方面若两条部分路导出一个中间点 v，此时，只需考虑较短的部分路，即对应于较长的部分路在该点修剪该树，修剪算法如下.

修剪算法

设 G 为赋权有向无圈图，该算法求 G 中顶点 u 和 w 之间的最短路. 这个算法具有如下性质：

(a) 算法执行期间，G 的每个顶点 v' 被作两个指定

(1) 从 u 到 v' 的当前最短路的长度 $l(v')$.

(2) 从 u 到 v' 的长为 $l(v')$ 的路 $p(v')$.

(b) 最初，设 $l(u)=0, p(u)=u$. 每个其他点 v 初始化指定 $l(v)=\infty, p(v)=\varnothing$.

(c) 算法的每一步检查从 v' 到 v 的边 $e=(v',v)$，设长度为 k. 计算 $l(v')+k$.

(1) 若 $l(v')+k<l(v)$，则找到从 u 到 v 的更短路. 于是刷新：

$$l(v)=l(v')+k, \text{且 } p(v)=p(v')v.$$

[当 $l(v)=\infty$ 时，即首次进入 v 时条件总成立.]

(2) 否则，不改变 $l(v)$ 和 $p(v)$.

若没有未检查的边进入 v，则称 $p(v)$ 已确定.

(d) 当 $p(w)$ 已确定时，算法结束.

注 若 v' 先前已访问，即 $p(v')\neq\varnothing$，则(c)中的边 $e=(v',v)$ 才能被选择. 进一步，通常最

好检查开始于 v'，且路 $p'(v)$ 已确定的边.

例 9.13 对图 9－19(a)中的图 G 用修剪算法.

从 u 起：相继点为 x，y 和 z，它们都是首次进入，于是

(1) 置 $l(x)=4$，$p(x)=ux$.

(2) 置 $l(y)=6$，$p(y)=uy$.

(3) 置 $l(z)=2$，$p(z)=uz$.

注意到 $p(x)$ 和 $p(z)$ 都已确定.

从 x 起：相继点为 r 和 y，其中 r 为首次进入，于是.

(1) 置 $l(r)=4+4=8$，且 $p(r)=p(x)\ r=uxr$.

(2) 计算

$$l(x)+k=4+3=7，不小于\ l(y)=6.$$

于是留下 $l(y)$ 和 $p(y)$.

注意到 $p(r)$ 已经确定.

从 z 起：相继点为 t 和 y，其中 t 为首次进入，于是

(1) 置 $l(t)=l(z)+k=2+5=7$，且 $p(t)=p(z)t=uzt$.

(2) 计算

$$l(z)+k=2+3=5，小于\ l(y)=6.$$

已发现到 y 的更短路，因此刷新 $l(y)$ 和 $p(y)$，即，置 $l(y)=l(z)+k=5$，且 $p(y)=p(z)y=uzy$.

注意到 $p(y)$ 已确定.

从 y 起：相继点为 s 和 t，其中 s 为首次进入. 于是，

(1) 置 $l(s)=l(y)+k=5+2=7$，且 $p(s)-p(y)s=uzys$.

(2) 计算

$$l(y)+k=5+1=6，小于\ l(t)=7.$$

于是，改变 $l(t)$ 和 $p(t)$，

$l(t)=l(y)+1=6$ 且 $p(t)=p(y)t=uzyt$.

注意到 $p(t)$ 已确定.

从 r 起：相继点为 w 和 s，其中 w 为首次进入. 于是

(1) 置 $l(w)=l(r)+3=11$，且 $p(w)=p(r)w=uxrw$.

(2) 计算

$$l(r)+k=8+2=10，不小于\ l(s)=7.$$

于是，留下 $l(s)$ 和 $p(s)$.

注意到 $p(s)$ 已确定.

从 s 起：相继点为 w，计算

$$l(s)+k=7+3=10，小于\ l(w)=11.$$

于是，改变 $l(w)$ 和 $p(w)$.

$$l(w)=l(s)+3=10，且\ p(w)=p(s)w=uzysw.$$

从 t 起：相继点为 w，计算

$$l(t)+k=6+3=9，小于\ l(w)=10.$$

于是，改变 $l(w)$ 和 $p(w)$.

$$l(w)=l(t)+3=9，且\ p(w)-p(t)w=uzytw.$$

目前 $p(w)$ 已确定.

由于 $p(w)$ 已确定，所以算法终止. 因此

$$p(w)=uzytw$$

是从 u 到 w 的最短路，且 $l(w)=9$.

上面例子中检查的边构成了图 9-20 中的有根树. 这是图 9-19(b)中的树，该树在属于更长部分路的顶点被修剪. 注意到该树原有的 23 条边只需检查 13 条边.

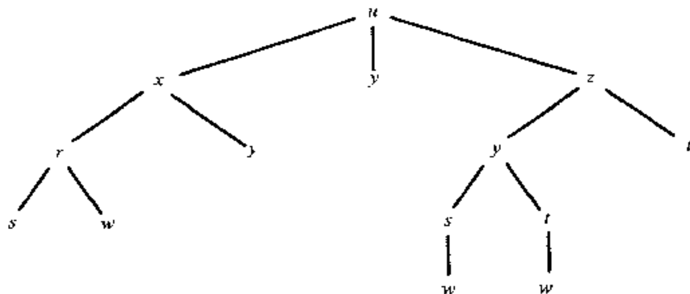


图 9-20

问题与解答

图术语

9.1　考虑图 9-21 中的有向图 G.

(a) 正式描述 G.

(b) 求从 X 到 Z 的所有简单路.

(c) 求从 Y 到 Z 的所有简单路.

(d) 求 G 的所有圈.

(e) G 单侧连通吗? 强连通吗?

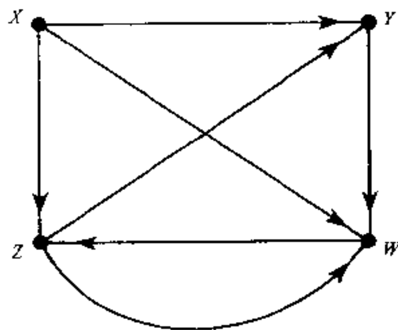


图 9-21

解 ☞　(a) 顶点集 V 有 4 个顶点，边集 E 有以下 7 条(有向)边：

$$V=\{X,Y,Z,W\},$$

$E=\{(X,Y),(X,Z),(X,W),(Y,W),(Z,Y),(Z,W),(W,Z)\}$.

(b) 从 X 到 Z 有 3 条简单路.

$$(X,Z),(X,W,Z)\text{和}(X,Y,W,Z).$$

(c) 从 Y 到 Z 只有一条简单路(Y,W,Z).

(d) G 中只有一个圈(Y,W,Z,Y).

(e) G 是单侧连通的，因为(X,Y,W,Z)为支撑路. G 不是强连通的，因为没有闭支撑路.

9.2　考虑图 9-21 中的有向图 G.

(a) 求 G 的每个顶点的入度和出度.

(b) 求 G 的每个顶点的相继点列表.

(c) 存在发点或收点吗?

(d) 求 G 的由顶点集 $V'=\{X,Y,Z\}$确定的子图 H.

解 ☞　(a)计算终于和起于顶点 v 的边数就分别得到 indeg(v)和 outdeg(v)，有如下数据.

$$\text{indeg}(X)=0,\quad \text{indeg}(Y)=2,\quad \text{indeg}(Z)=2,\quad \text{indeg}(W)=3,$$
$$\text{outdeg}(X)=3,\quad \text{outdeg}(Y)=1,\quad \text{outdeg}(Z)=2,\quad \text{outdeg}(W)=1.$$

(正如所料，入度之和与出度之和都等于边数 7.)

(b) 对 G 的每条边(u,v)，添加 v 到 u 的相继列表 succ(u). 于是，有

$$\text{succ}(X)=[Y,Z,W],\ \text{succ}(Y)=[W],\ \text{succ}(Z)=[Y,W],\ \text{succ}(W)=[Z]$$

(c) X 是发点，因为没有边进入 X. 即 indeg(X)=0. 没有收点，因为每个顶点都是一条边的起点. 即每个点有非零出度.

(d) 设 E'为 G 的端点在 V'中的边的集合，即 $E'=\{(X,Y),(X,Z),(Z,Y)\}$，则 $H=H(V',E')$.

9.3　考虑图 9-22 中的有向图.

(a) 求从 v_1 到 v_6 的两条简单路. $\alpha=(v_1,v_2,v_4,v_6)$是这样的简单路吗?

(b) 求 G 的含有 v_3 的所有圈.

(c) G 单侧连通吗? 强连通吗?

解 ☞ (a) 简单路是所有点互不相同的路,于是,(v_1,v_5,v_6)和(v_1,v_2,v_3,v_5,v_6)是两条从 v_1 到 v_6 的简单路. 由于连接 v_4 和 v_6 的边不起于 v_4,所以序列 α 甚至不是路.

(b) 有两个这样的圈:(v_3,v_1,v_2,v_3)和$(v_3,v_5,v_6,v_1,v_2,v_3)$.

(c) G 是单侧连通的,因为$(v_1,v_2,v_3,v_5,v_6,v_4)$是支撑路. G 不是强连通的,因为没有闭支撑路.

9.4 考虑图 9-22 中的有向图.

(a) 求 G 的每个顶点的相继列表.

(b) G 有发点吗? 有收点吗?

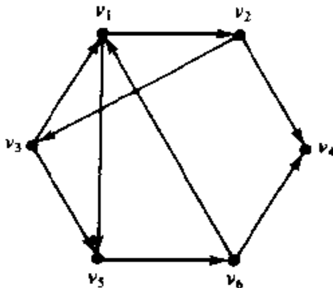


图 9-22

解 ☞ (a)对 G 的每条边(u,v)添加 v 到 u 的相继列表 $\mathrm{succ}(u)$,得到:

$\mathrm{succ}(v_1)=[v_2,v_5]$, $\mathrm{succ}(v_2)=[v_3,v_4]$,

$\mathrm{succ}(v_3)=[v_1,v_5]$, $\mathrm{succ}(v_4)=\varnothing$,

$\mathrm{succ}(v_5)=[v_6]$, $\mathrm{succ}(v_6)=[v_1,v_4]$.

(正如所料,相继点数为 9,即为边数)

(b) 没有发点,因为每个顶点都是某条边的端点:只有 v_4 为收点,因为没有边起于 v_4.即,$\mathrm{succ}(v_4)=\varnothing$,空集.

9.5 考虑下面的有向图 G:

$$V(G)=\{a,b,c,d,e,f,g\},$$

$$E(G)=\{(a,a),(b,e),(a,e),(e,b),(g,c),(a,e),(d,f),(d,b),(g,g)\},$$

(a) 确定环与平行边.

(b) G 中有发点吗?

(c) G 中有收点吗?

(d) 求 G 的由顶点集 $V'=\{a,b,c,d\}$确定的子图 H.

解 ☞ (a) 环是具有相同起点和终点的边. 因此,(a,a)和(g,g)是环. 若两条边具有相同的起点和终点. 则称为平行边. 因此,(a,e)和(a,e)为平行边.

(b) 顶点 d 是发点. 因为没有边终止于 d,即 d 不作为任何边的第二个元素出现. 没有其他的发点.

(c) c 和 f 都是收点. 因为没有边起于 c 或 f. 即 c 与 f 都不作为任何边的第一个元素出现. 没有其他的收点.

(d) 设 E'由 G 的端点位于 $V'=\{a,b,c,d\}$的边组成,则 $E'=\{(a,a),(d,b)\}$. 于是 $H=H(V',E')$.

9.6 设 G 为有向图,顶点集 $V(G)=\{a,b,c,d,e\}$,后继列表为

$$\mathrm{succ}(a)=[b,c],\quad \mathrm{succ}(b)=\varnothing\quad \mathrm{succ}(c)=[d,e],$$
$$\mathrm{succ}(d)=[a,b,e],\quad \mathrm{succ}(e)=\varnothing.$$

(a) 列出 G 的边(于是 G 由其后继列表确定).

(b) G 是弱连通的吗? 单侧连通? 强连通?

解 ☞ (a)当 $y\in \mathrm{succ}(x)$,则有一条边(x,y),于是

$$E(G)=\{(a,b),(a,c),(c,d),(c,e),(d,a),(d,b),(d,e)\}.$$

(b) 由于 b 和 e 为收点,所以从 b 到 e,或从 e 到 b 没有路. 于是,G 既不是单侧连通的,也不是强连通的. 不过,G 是弱连通的,因为(c,a,b,d,e)为支撑半路.

有根树,有序有根树

9.7 考虑图 9-23 中的有根树 T.

(a) 确定从根 R 到下列每个顶点的路 α,并求该点的层次 n: (i) H;(ii) F;(iii) M.

(b) 求 E 的兄弟.

(c) 求 T 的树叶.

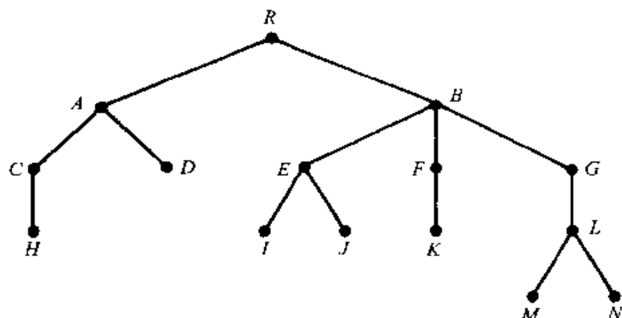


图 9－23

解答 (a) 列出沿树从 R 向下检查到该点的顶点. 除 R 外的顶点数，就是层次：

(i) $\alpha=(R,A,C,H)$，$n=3$；(ii) $\alpha=(R,B,F)$，$n=2$；(iii) $\alpha=(R,B,G,L,M)$，$n=4$.

(b) E 的兄弟为 F 和 G，因为它们共有同一个父亲 B.

(c) 树叶是没有孩子的顶点，即 H,D,I,J,K,M,N.

9.8 考虑典型的商业情形，在两个主要地区出售其产品的某公司准备推出新产品，推出产品的通常程序如下. 首先，在区域Ⅰ的一个很小的试验市场推出产品，若产品不成功，则停止；若产品成功，则在区域Ⅰ推广. 若在区域Ⅰ推广成功，再在区域Ⅱ推出；若不成功，则在区域Ⅱ的一个小试验市场推出. 再一次，若成功，则在整个区域推出. 用一棵树来表示推出产品程序的各种可能结果.

解答 在图 9－24 中用树描述了可能的结果，有四个可能的结果，用从根到该树的树叶的四个树枝表示(这里根在树的左边)：

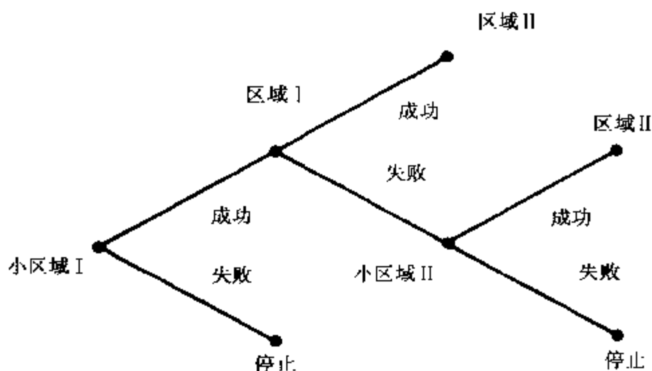


图 9－24

(1) 产品在区域Ⅰ的最初的小市场不成功，停止.

(2) 产品在最初的小试验市场成功，且在区域Ⅰ成功，并在区域Ⅱ推出.

(3) 产品在最初试验市场成功，但在区域Ⅰ并不成功，它在区域Ⅱ的小试验市场，也不成功，停止.

(4) 产品在最初的试验市场成功，但在区域Ⅰ并不成功，在区域Ⅱ的小试验市场也成功，因而在区域Ⅱ推出.

9.9 图 9－25 给出一棵有序根树 T，其顶点用通用地址系统标号. 求该树 T 的地址的字典序.

解答 由于有序根树通常画成如图 9－25 一样，使得边从左到右排序，所以记下最左的枝，再记下左第二枝，等等就可得到字典序. 因此，记下 T 的最左枝得：

$$0,\ 1,\ 1.1,\ 1.1.1.$$

接下来的一枝为 1.2. 因此，添加 1.2 得

$$0,\ 1,\ 1.1,\ 1.1.1,\ 1.2.$$

类似地，添加下一枝

$$1.3,\ 1.3.1,\ 1.3.1.1.$$

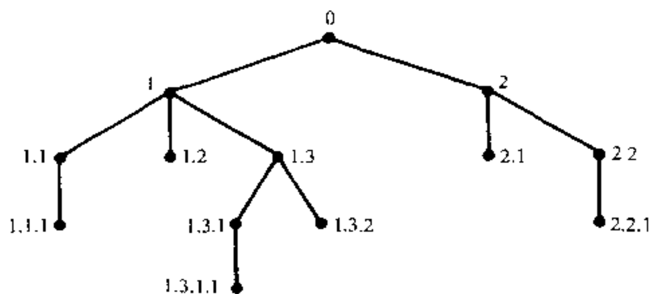


图 9 - 25

如此继续,得

0, 1, 1.1, 1.1.1, 1.2. 1.3, 1.3.1, 1.3.1.1, 1.3.2, 2, 2.1, 2.2, 2.2.1.

9.10 考虑下列随机顺序排放的地址.

1, 2.2.1, 3.2, 2.2.1.1, 1.1.1, 0, 2.1, 3.2.1.1,

3, 3.1, 2.2, 2.1.1, 3.2.1, 1.1, 3.2.1.2, 2, 1.1.2.

(a) 以字典序排放地址.

(b) 画出相应的有序根树.

解 ☞ (a) 地址的字典序如下:

0, 1, 1.1, 1.1.1, 1.1.2, 2, 2.1, 2.1.1, 2.2, 2.2.1,

2.2.1.1, 3, 3.1, 3.2, 3.2.1, 3.2.1.1, 3.2.1.2.

(b) 为画出具有给定字典序的树 T. 从最左的枝开始,然后紧靠它添加枝,等等. 因此,画根 0,枝 1,枝 1.1,枝 1.1.1. 由于 2 在树中不紧随 1.1.1,所以,这是下一枝的开始,为 2,2.1, 2.1.1. 如此继续便得图 9 - 26 中的树.

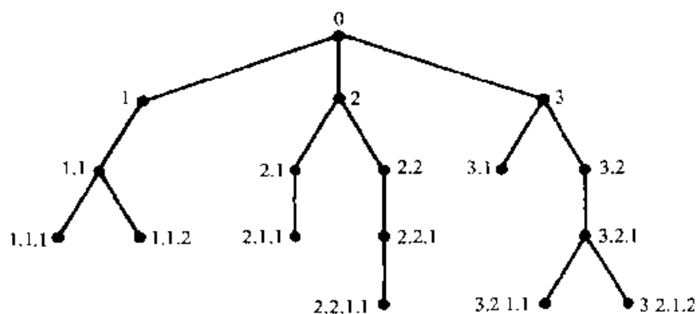


图 9 - 26

图的序列表示

9.11 考虑图 9 - 21 中的图 G,假设顶点以下面的数组 DATA 存贮.

DATA: X, Y, Z, W.

(a) 求图 G 的邻接矩阵 A.

(b) 用邻接矩阵 A 的幂求 G 的路矩阵 P.

(c) G 强连通吗?

解 ☞ (a) 顶点通常按其在存贮中的出现排序. 即设 $v_1=X, v_2=Y, v_3=Z, v_4=W$. G 的邻接矩阵 A 如下:

$$A=\begin{bmatrix}0&1&1&1\\0&0&0&1\\0&1&0&1\\0&0&1&0\end{bmatrix}.$$

这里,若有从 v_i 到 v_j 的边,则 $a_{ij}=1$. 否则 $a_{ij}=0$.

(b) 因G有4个顶点，计算A^2，A^3，A^4及$B_4=A+A^2+A^3+A^4$：

$$A^2=\begin{bmatrix}0&1&1&2\\0&0&1&0\\0&0&1&1\\0&1&0&1\end{bmatrix},\quad A^3=\begin{bmatrix}0&1&2&2\\0&1&0&1\\0&1&1&1\\0&0&1&1\end{bmatrix},$$

$$A^4=\begin{bmatrix}0&2&2&3\\0&0&1&1\\0&1&1&2\\0&1&1&1\end{bmatrix},\quad B_4=\begin{bmatrix}0&5&6&8\\0&1&2&3\\0&3&3&5\\0&2&3&5\end{bmatrix}.$$

路矩阵P可这样得到，当矩阵B_4中有一个非零值，则令$P_{ij}=1$. 于是，

$$P=\begin{bmatrix}0&1&1&1\\0&1&1&1\\0&1&1&1\\0&1&1&1\end{bmatrix}.$$

(c) 路矩阵表明没有从v_2到v_1的路，事实上，没有从任何点到v_1的路. 因此，G不是强连通的.

9.12 考虑图9-21中图G的邻接矩阵A，在A问题9.11中得到. 利用Warshall算法而不是A的幂求G的路矩阵P.

解 计算矩阵P_0，P_1，P_2，P_3和P_4，这里$P_0=A$，且

$$P_k[i,j]=P_{k-1}[i,j]\vee(P_{k-1}[i,k]\wedge P_{k-1}[k,j])$$

即

若$P_{k-1}[i,j]=1$，或$P_{k-1}[i,k]=1$且$P_{k-1}[k,j]=1$，则$P_k[i,j]=1$.

则

$$P_1=\begin{bmatrix}0&1&1&1\\0&0&0&1\\0&1&0&1\\0&0&1&0\end{bmatrix},\quad P_2\begin{bmatrix}0&1&1&1\\0&0&0&1\\0&1&0&1\\0&0&1&0\end{bmatrix},$$

$$P_3=\begin{bmatrix}0&1&1&1\\0&0&0&1\\0&1&0&1\\0&1&1&1\end{bmatrix},\quad P_4=\begin{bmatrix}0&1&1&1\\0&1&1&1\\0&1&1&1\\0&1&1&1\end{bmatrix}.$$

注意到$P_0=P_1=P_2=A$，基于下面的原因，P_3改变了.

$P_3(4,2)=1$，因为$P_2(4,3)=1$，且$P_2(3,2)=1$.

$P_3(4,4)=1$，因为$P_2(4,3)=1$，且$P_2(3,4)=1$.

类似地，P_4改变了. 最后的矩阵P_4就是所需的图G的路矩阵P.

9.13 画赋权图G的示意图，图G用下面的点组DATA以及权矩阵W存贮.

$$\text{DATA}: X,Y,S,T;\ W=\begin{bmatrix}0&0&3&0\\5&0&1&7\\2&0&0&4\\0&6&8&0\end{bmatrix}.$$

解 示意图见图9-27. 顶点以DATA中的值标号. 并且若$w_{ij}\neq0$，则存在从v_i到v_j且权为w_{ij}的边.（假设$v_1=X$，$v_2=Y$，$v_3=S$，$v_4=T$，顶点在组DATA中的次序）.

9.14 证明命题9.4：设A为图G的邻接矩阵，则矩阵A^k中的第i行第j列的元素$a_k(i,j)$就是从v_i到v_j的长为k的路的条数.

证 对k用归纳法证明. 首先注意到从v_i到v_j的长为1的路恰为边(v_i,v_j). 由邻接矩阵A的定义，$a_1(i,j)=a_{ij}$为从v_i到v_j的边数. 因此，命题对$k=1$成立.

假设$k>1$.（设G有m个顶点.）因$A^k=A^{k-1}\cdot A$，故

$$a_k(i,j)=\sum_{s=1}^{m}a_{k-1}(i,s)a_1(s,j).$$

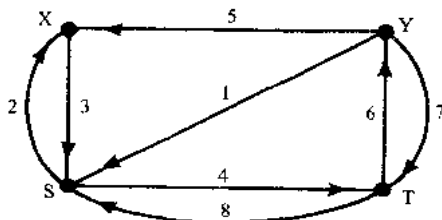


图 9－27

由归纳假设，$a_{k-1}(i,s)$为从 v_i 到 v_s 的长为$k-1$ 的路的条数，而 $a_1(s,j)$为从 v_s 到 v_j 长为 1 的路的条数. 于是 $a_{k-1}(i,s)a_1(s,j)$为从 v_i 到 v_j 的长为 k 的路的条数. 这里 v_s 为紧靠最后点的顶点. 因此，从 v_i 到 v_j 的长为 k 的所有路可对所有 s 相加 $a_{k-1}(i,s)a_1(s,j)$得到. 即 $a_k(i,j)$为从 v_i 到 v_j 的长为 k 的路的条数. 由此命题得证.

图的链表示

9.15 赋权图 G 有 6 个顶点 A、B，…，F，且用如图 9－28 的点文件和边文件的链表示存贮.

(a) 按它们在存贮中的次序列出其顶点.

(b) 求每个点 v 的后继列表 succ(v)

点文件

START 3

	1	2	3	4	5	6	7	8
VERTEX	D		B	F	A		C	E
NEXT-V	7		1	5	0		8	4
PTR	9		3	0	6		10	1

边文件

	1	2	3	4	5	6	7	8	9	10
BEG-V	8	5	3		5	5	3		1	7
END-V	1	4	7		3	1	1		8	8
NEXT-E	0	5	7		0	2	0		0	0
WEIGHT	3	4	2		6	3	1		2	5

图 9－28

解 (a) 由于 START=3，故列表以顶点 B 开头，然后 NEXT-V 指向 1(D)，再7(C)，再 8(E)，再 4(F)，再 5(A)，即

$$B,D,C,E,F,A.$$

(b) 这里 succ(A)=[1(D)，4(F)，3(B)]=[D,F,B]. 特别地，因 PTR [5(A)]=6，且 END-V[6]=1(D)，故 succ(A)以 D 开头. 由 NEXT-E[6]=2 与 END-V[2]=4[F]知 F 为 Succ(A)中的下一个顶点. 再由 NEXT-E[2]=5 与 END-V[5]=3(B)知 B 为 succ(A)中的下一个顶点. 然而，由 NEXT-E[5]=0 知 A 没有更多的后继. 类似地，

$$\text{succ}(B)=[C,D],\ \text{succ}(C)=[E],\ \text{succ}(D)=E,\ \text{succ}(E)=[D].$$

进一步 succ(F)=∅，因为 PTR[4(F)]=0. 综上，

$$G=[A:D,F,B;B:C,D;C:E;D:E;E:D;F:\varnothing].$$

9.16 考虑赋权图 G，其链表示如图 9－28. 画出图 G.

解 利用问题 9.15(b)中得到的后继列表以及图 9－28 中边文件中各边的权可画得图 G，如图 9－29.

9.17 设图 G 由下表给出：

$$G=[X:Y,Z,W;\ Y:X,Y,W;\ Z:Z,W;\ W:Z].$$

(a) 求 G 中的顶点数与边数.

(b) 有发点或收点吗?

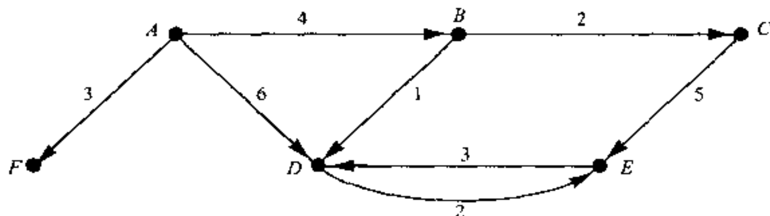


图 9-29

(c) 画出图 G.

解 (a) 由表可知,G 有四个顶点 X,Y,Z,W,且顶点的出度分别为 3,3,2,1. 因此,有 $3+3+2+1=9$ 条边.

(b) 没有零出度顶点,因而没有收点. 又每个顶点都是后继点,因而没有发点.

(c) 利用邻接列表,画图 G,如图 9-30.

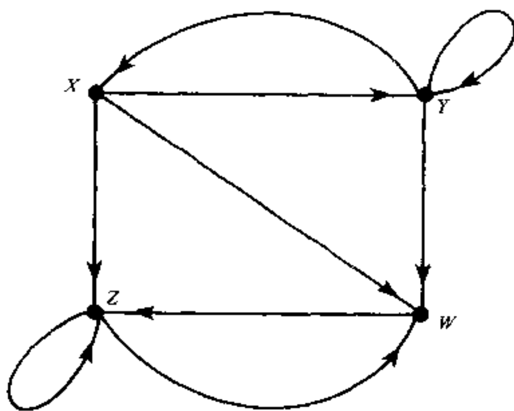


图 9-30

9.18 设友谊航空公司每日有以下 9 个航班:

103	从 Atlanta 到 Houston	106	从 Houston 到 Atlanta
201	从 Boston 到 Chicago	203	从 Boston 到 Denver
204	从 Denver 到 Boston	301	从 Denver 到 Reno
305	从 Chicago 到 Miami	308	从 Miami 到 Boston
401	从 Reno 到 Chicago		

借助标号有向图描述这些数据.

解 用图 9-31 中的图 G 描述这些数据(为方便省略航班号).

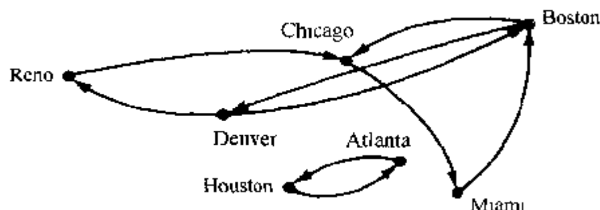


图 9-31

9.19 描述问题 9.18 中的图 G 如何用链表示存贮. 这里城市与航班以线性排序组出现.

解 如图 9-32(这里 $A,B,\cdots$ 分别表示 Atlanta,Boston,$\cdots$). 注意到 START 变量是不必要的,因为各城市构成一个组而不是链表. 并用 ORIG(出发地)和 DEST(目的地)代替 BEG-V 和 END-V.

点文件

	1	2	3	4	5	6	7	8
CITY	A	B	C	D	H	M	R	
PTR	1	3	7	5	2	8	9	

边文件

	1	2	3	4	5	6	7	8	9	10
NUMBER	103	106	201	203	204	301	305	308	402	
ORIG	1	5	2	2	4	4	3	6	7	
DEST	5	1	3	4	2	7	6	2	3	
NEXT-E	0	0	4	0	6	0	0	0	0	

图 9－32

9.20 明显地，问题 9.18 中的数据可有效地存贮在这样的文件中，每个记录仅含三个字段.航班号，出发地，目的地.不过，当有许多许多航班时，这样的表示就不容易回答下面自然的问题：

(i) 存在从城市 X 到 Y 的直航吗？

(ii) 人们可以从城市 X 到 Y 吗？

(iii) 从城市 X 到 Y 的最直接(逗留最少)的路线是什么？

证明若数据由如图 9－32 中的图的链表示存贮，则比方说，(ii)的答案如何更容易得到.

解 ☞ 回答(ii)的一种方法是用广度优先查找或深度优先查找算法确定城市 Y 从城市 X 是否从城市 Z 可达.这样的算法需要邻接列表，它可从图的链表示中轻易地得到.但不能从仅用三个字段的上面的表示得到.

杂题

9.21 画出对应于下面的非负整数的邻接矩阵 A 的多重图 G.

$$A=\begin{bmatrix}0 & 2 & 0 & 1\\ 0 & 0 & 1 & 1\\ 2 & 1 & 1 & 0\\ 0 & 0 & 1 & 1\end{bmatrix}.$$

解 ☞ 因为 A 为 4×4 矩阵，所以 G 有 4 个顶点，设为 v_1, v_2, v_3, v_4，对每个 a_{ij}，画从 v_i 到 v_j 的 a_{ij} 条弧(有向边)，得到图 9－33 中的图即为 G.

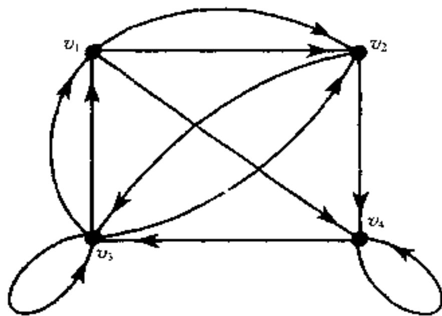


图 9－33

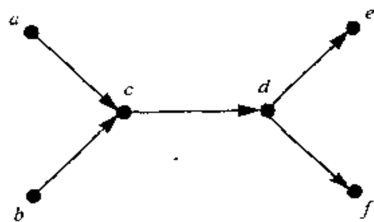


图 9－34

9.22 考虑图 9－34 中的无圈有向图 S.求 S 的所有可能的拓扑排序.

解 ☞ S 有四个可能的拓扑排序.特别地，每个拓扑排序 T 必起于 a 或 b，必终于 e 或 f.且 c 和 d 必分别为第三，第四个元素.这四个排序如下：

$$T_1=[a,b,c,d,e,f],\qquad T_2=[b,a,c,d,e,f],$$
$$T_3=[a,b,c,d,f,e],\qquad T_4=[b,a,c,d,f,e].$$

补　充　题

图术语

9.23 考虑图 9 - 35 的图 G.

(a) 求每个顶点的入度和出度.

(b) 有发点或收点吗?

(c) 求从 v_1 到 v_4 的所有简单路.

(d) 求 G 中的所有圈.

(e) 求从 v_1 到 v_3 的所有长不超过 3 的路.

(f) G 单侧连通吗? 强连通吗?

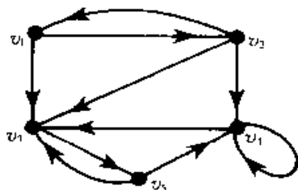


图 9 - 35

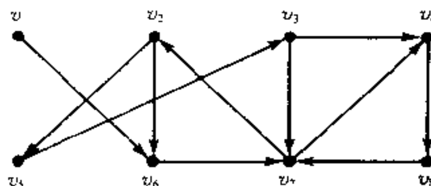


图 9 - 36

9.24 考虑图 9 - 36 中的图 G.

(a) 有发点或收点吗?

(b) 求从 v_1 到 v_4 的所有简单路.

(c) 求从 v_1 到 v_4 的一条非简单路.

(d) 求 G 中含 v_4 的所有圈.

9.25 考虑图 9 - 36 中的图 G.

(a) 求 $\text{succ}(v_1)$, $\text{succ}(v_3)$, $\text{succ}(v_5)$, $\text{succ}(v_7)$.

(b) 求 G 的由(i) $\{v_1, v_3, v_5, v_6\}$. (ii) $\{v_2, v_3, v_5, v_7\}$生成的子图 H.

9.26 考虑图 G,这里

$V(G)=\{A,B,C,D,E\}$ 且 $E(G)=\{(A,D),(B,C),(C,E),(D,B)(D,D),(D,E),(E,A)\}$.

(a) 用邻接表描述 G.

(b) G 有环或平行边吗?

(c) 求从 D 到 E 的所有简单路.

(d) 求 G 中的所有圈.

(e) G 单侧连通吗? 强连通吗?

(f) 求 G 的顶点为 C,D,E 的子图个数.

(g) 求 G 的由 C,D,E 生成的子图 H.

9.27 考虑图 9 - 37 中的图.

(a) 用邻接表描述 G.

(b) G 有发点或收点吗?

(c) 求从 A 到 E 的所有简单路.

(d) 求 G 的所有圈.

(e) 用给出 G 的支撑路的方法证明 G 是单侧连通的.

(f) G 强连通吗?

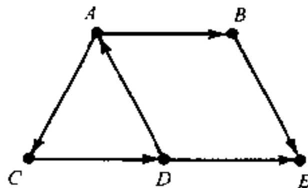


图 9 - 37

9.28 画一个代表下列情况的标号图 G. 三姐妹 Barbara,Rose 与 Susan 每人定期给她们的妈妈 Gertrude 打电话,而 Gertrude 只打电话给 Rose. Susan 不打电话给 Rose,而 Rose 还是给 Susan 打电话. Barbara 与 Susan 相互打电话,Barbara 与 Rose 也相互打电话.

9.29 设 R 为由 $V=\{2,3,4,9,15\}$上的"x 小于 y 且 x 与 y 互素"定义的关系(有向图). (a) 画出图 R 的示意图. (b) R 弱连通吗? 单侧连通吗? 强连通吗?

9.30 设 G 为有向图. 若对每对不同顶点 u 和 v,或者(u,v)是一条弧,或者(v,u)是一条弧. 则称 G 为完全的,

证明有限完全有向图 G 有一条含所有顶点的路.(这对无向完图度显然成立.)由此 G 是单侧连通的.

有根树,有序根树

9.31 考虑图 9-38 的有根树 T.

(a) 确定从根 R 到下面每个顶点的路 α,并求该顶点的层次:(i) D; (ii) J; (iii) G.

(b) 求 T 的树叶.

(c) 设 T 为有序根树,求 T 的每个树叶的通用地址.

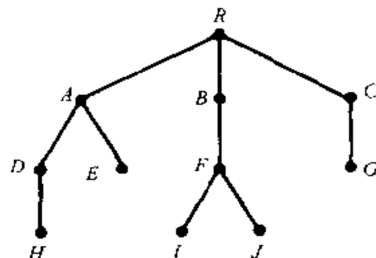


图 9-38

9.32 下面是按随机顺序排放的地址.

2.1.1, 3.1, 2.1, 1, 2.2.1.2, 0, 3.2, 2.2, 1.1, 2, 3.1.1, 2.2.1, 3, 2.2.1.1.

(a) 以字典序排放这些地址.

(b) 画出相应的有根树.

9.33 考虑代数式

$$E=\frac{(3x-5z)^4}{a(2b+c^2)}.$$

(a) 用箭头 ↑ 表示指数,星号 * 表示乘法,斜杠/表示除法,画出相应的有序根树 T.

(b) 用 T 将 E 改写成波兰前缀形式.

图的序列表示

9.34 考虑图 9-39 中的图 G.

(a) 求 G 的邻接矩阵 A 和路矩阵 P,

(b) 对所有的 $k>0$,求 n_k,这里 n_k 表示从 v_1 到 v_4 的长为 k 的路的条数,

(c) G 弱连通吗?单侧连通吗?强连通吗?

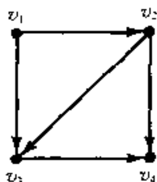


图 9-39

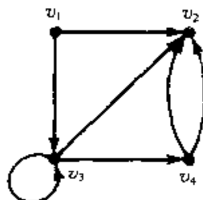


图 9-40

9.35 对图 9-40 中的图重复问题 9.34.

9.36 设 P 为图 G 的路矩阵,当(a) G 强连通时,(b) G 单侧连通时,描述 P.

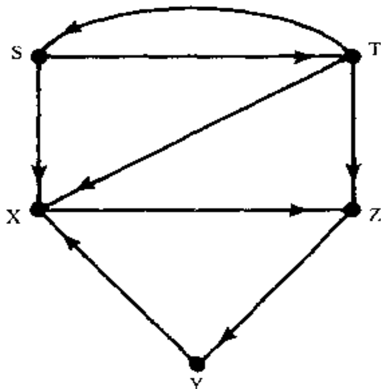


图 9-41

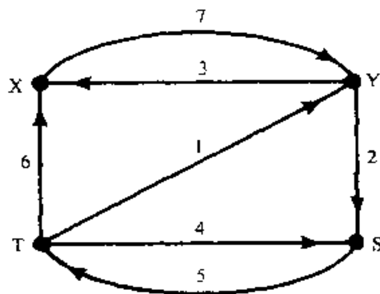


图 9-42

9.37 考虑图 9-41 中的图 G. 这里顶点用组 DATA:X,Y,Z,S,T 存贮.

(a) 求 G 的邻接矩阵 A 和路矩阵 P.

(b) 求 G 中的所有圈.

(c) G 单侧连通吗？强连通吗？

9.38 考虑图 9 - 42 中的赋权图 G，顶点用组 DATA：X,Y,S,T 存贮.

(a) 求 G 的权矩阵 W.

(b) 用 Warshall 算法求最短路的矩阵 Q.

9.39 假设图 G 用一个整数 M，表示顶点 $1,2,\cdots,M$，以及代表 G 的边的 N 个有序整数对的列表存贮. 编制程序解决下列问题.

(a) 求图 G 的 $M\times M$ 阶邻接矩阵 A.

(b) 用 A 及 Warshall 算法求 G 的路矩阵 P.

用下面的数据检测上面的程序：

(i) $M=5;N=8;(3,4),(5,3),(2,4),(1,5),(3,2),(4,2),(3,1),(5,1)$.

(ii) $M=6;N=10;(1,6)(2,1),(2,3),(3,5),(4,5),(4,2),(2,6),(5,3),(4,3),(6,4)$.

9.40 设图 G 用一个整数 M，代表顶点 $1,2,\cdots,M$，以及 N 个整数的有序三元组 (a_i,b_i,w_i) 的列表作为输入，其中 (a_i,b_i) 为 G 的边，w_i 为它的权，编制程序解决下列问题：

(a) 求图 G 的 $M\times M$ 阶权矩阵 W.

(b) 用 A 及 Warshall 算法求 G 的顶点间最短路的矩阵 Q.

用下面的数据检测上面的程序.

(i) $M=4;N=7;(1,2,5),(2,4,2),(3,2,3),(1,1,7),(4,1,4),(4,3,1)$.

(ii) $M=5;N=8;(3,5,3),(4,1,2),(5,2,2),(1,5,5),(1,3,1),(2,4,1),(3,4,4),(5,4,4)$.

图的链表示

9.41 六个顶点 $A,B,\cdots,F$ 的赋权图用图 9 - 43 中的一个点文件与边文件的链表示存贮.

(a) 按存贮出现的次序列出顶点.

(b) 对每个顶点 v，求其后继列表 succ(v).

点文件

START [7]

	1	2	3	4	5	6	7	8
VERTEX	D		B	F	A		C	E
NEXT-V	3		8	1	0		4	5
PTR	7		5	9	2		3	0

边文件

	1	2	3	4	5	6	7	8	9	10	11	12
BEG-V	5	5	7		3	7	1		4	1	4	7
END-V	8	7	5		1	1	5		8	4	3	8
NEXT-E	0	1	12		0	0	10		11	0	0	6
WEIGHT	5	2	1		3	2	4		1	3	4	1

图 9 - 43

9.42 考虑赋权图 G，其链表示如图 9 - 43，画出图 G.

9.43 设图 G 由下表给出：

$$G=[A:B,C;\ B:C,D;\ C:C;\ D:B;\ E:\varnothing].$$

(a) 求 G 的顶点数与边数.

(b) 有发点或收点吗？

(c) 画出 G 的图.

(d) G 弱连通吗？单侧连通吗？强连通吗？

9.44 对下表重复问题 9.43.

$$G=[A:D;\ B:C;\ C:E;\ D:B,D,E;\ E:A].$$

9.45 对下表重复问题 9.43.

$$G=[A:B,C,D,F;\ B:E;C:\varnothing;\ D:\varnothing;\ E:B,D,G;\ F:D,G;\ G:D].$$

9.46 假设友谊航空公司每天有 8 个航班服务 7 个城市. Atlanta，Boston，Chicago，Denver，Houston，Philadelphia 与 Washington，并设航班数据如图 9 - 44 存贮，即用城市与航班的线性排序组的链表示存贮. 画一

个表述这些数据的标号有向图.

点文件

	1	2	3	4	5	6	7	8
CITY	A	B	C	D	H	P	W	
PTR	1	2	3	8	9	5	7	

边文件

	1	2	3	4	5	6	7	8	9	10
NUMBER	101	102	201	202	203	301	302	401	402	
ORIG	1	2	3	1	6	6	7	4	5	
DEST	2	3	6	7	3	1	6	5	4	
NEXT-E	4	0	0	0	6	0	0	0	0	

图 9 - 44

9.47 用图 9 - 44 的数据编制程序,其输入为 CITYX 与 CITYY. 若存在的话,则求出从城市 X 到城市 Y 的直航的航班号,用

(a) X=Atlanta,Y=Philadelphia; (b) X=Philadelphia, Y=Atlanta; (c) X=Houston, Y=Chicago; (d) X=Washington, Y=Chicago.

检测程序

9.48 用图 9 - 44 的数据编制程序,其输入为 CITYX 与 CITYY. 若存在的话,则求从城市 X 到城市 Y 的最直接的线路(最少逗留). 用问题 9.47 中的输入检测程序.

杂题

9.49 用修剪算法求图 9 - 45 中从 s 到 t 的最短路.

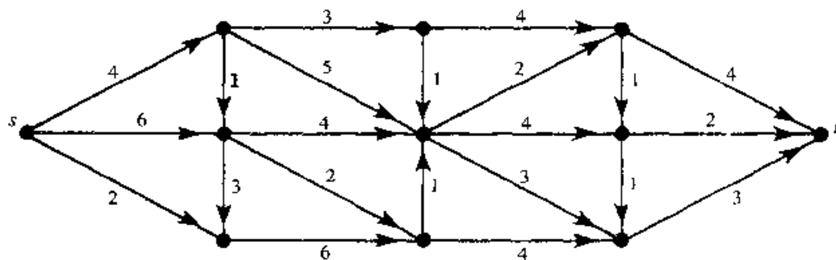


图 9 - 45

9.50 对下列每个图求其拓扑排序 T.

(a) $G=[A:Z;\ B:T;\ C:B;\ D:\varnothing;\ X:D;\ Y:X;\ Z:B,X;\ S:C,Z;\ T:\varnothing]$.

(b) $G=[A:X,Z;\ B:A;\ C:S,T;\ D:Y;\ X:S,T;\ Y:B;\ Z:\varnothing;\ S:Y;\ T:\varnothing]$.

(c) $G=[A:C,S;\ B:T,Z;\ C:\varnothing;\ D:Z;\ X:A;\ Y:A;\ Z:X,Y;\ S:\varnothing;\ T:Y]$.

补充题答案

9.23 (a) 入度:1,1,4,3,1; 出度:2,3,1,2,2.

(b) 无 (c) (v_1,v_2,v_4),(v_1,v_3,v_5,v_4), (v_1,v_2,v_3,v_5,v_4).

(d) (v_3,v_5,v_1,v_3). (e) (v_1,v_3),(v_1,v_2,v_3),(v_1,v_2,v_4,v_3);(v_1,v_2,v_1,v_3). (f) 单侧的,但不是强的.

9.24 (a) 发点:v_1. (b) (v_1,v_8,v_7,v_4), $(v_1,v_8,v_7,v_2,v_5,v_3,v_1)$. (c) $(v_1,v_8,v_7,v_2,v_5,v_7,v_1)$. (d) (v_4,v_8,v_7,v_4),$(v_4,v_8,v_7,v_2,v_5,v_3,v_4)$.

9.25 (a) succ(1)=[6], succ(3)=[4,7], succ(5)=[3], succ(7)=[2,4],(b) (i) (1,6), (5,3);(ii) (2,6), (6,7), (7,2),(3,7).

9.26 (a) $G=[A:D;B:C;C:E;D:B,D,E;E:A]$. (b) 环$(D,D)$.

(c) (D,E)，(D,B,C,E). (d) (A,D,E,A)，(A,D,B,C,E,A).

(e) 单侧的且为强的. (f)和(g)，H 有三条边：(C,E)、(D,E)，(D,D). 有 $8=2^3$ 种方法从这三条边中选取某些边，每个选取给出一个子图.

9.27 (a) $G=[A:B,C;\ B:E;\ C:D;\ D:A,E;\ E:\varnothing]$. (b) 收点：$E$. (c) (A,B,E)，(A,C,D,E).

(d) (A,C,D,A). (e) (C,D,A,B,E). (f) 否.

9.28 见图 9－46

9.29 (a) 见图 9－47. (b) 只是弱连通的.

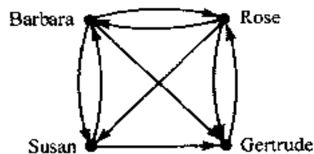


图 9－46

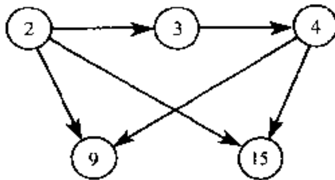


图 9－47

9.30 提示：设 $\alpha=(v_1,\cdots,v_m)$ 为 G 的最长路，且不含顶点 u. 若 (u,v_1) 为一条弧，则 $\beta=(u,\alpha)$ 延伸了 α，因此，(v_1,u) 是一条弧. 若 (u,v_2) 也是一条弧. 则 $\beta=(v_1,u,v_2,\cdots,v_m)$ 延伸 α，因此 (v_2,u) 是一条弧. 类似地，(v_3,u)，$\cdots$，(v_m,u) 为弧，因此，$\beta=(\alpha,u)$ 延伸 α. 与 α 的极大性矛盾.

9.31 (a)(i) (R,A,D)，2；(ii) (R,B,F,J)，3；(iii) (R,C,G)2.

(b) H,E,I,J,G. (c) H：1.1.1，E：1.2，I：2.1.1，J：2.1.2，G：3.1.

9.32 (a) 0，1，1.1，2，2.1，2.1.1，2.2，2.2.1，2.2.1.1，2.2.1.2，3，3.1，3.1.1，3.2.

(b) 见图 9－48.

9.33 (a) 见图 9－49. (b) $E=[/\uparrow - * 3x * 5z4 * a + * 2b \uparrow c2]$.

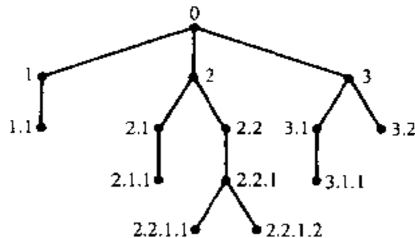


图 9－48

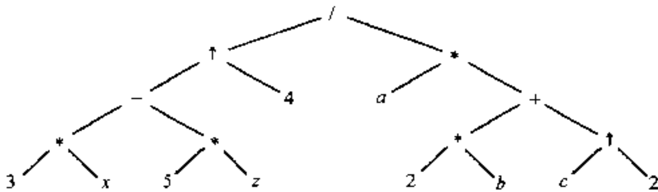


图 9－49

9.34 (a) $A=\begin{bmatrix}0&1&1&0\\0&0&1&1\\0&0&0&1\\0&0&0&0\end{bmatrix}$；$P=\begin{bmatrix}0&1&1&1\\0&0&1&1\\0&0&0&1\\0&0&0&0\end{bmatrix}$.

(b) 0，2，1，0，0，….

(c) 弱连通的，且为单侧连通的.

9.35 (a) $A=\begin{bmatrix}0&1&1&0\\0&0&0&0\\0&1&1&1\\0&2&0&0\end{bmatrix}$；$P=\begin{bmatrix}0&1&1&1\\0&0&0&0\\0&1&1&1\\0&1&0&0\end{bmatrix}$.

(b) 0，1，1，1，….

(c) 弱连通的，且为单侧连通的.

9.36 设 $P=[p_{ij}]$. 对 $i\neq j$，有(a) $p_{ij}\neq 0$，(b) 或 $p_{ij}\neq 0$ 或 $p_{ji}\neq 0$.

9.37 (a) $A=\begin{bmatrix}0&0&1&0&0\\1&0&0&0&0\\0&1&0&0&0\\1&0&0&0&1\\1&0&1&1&0\end{bmatrix}$；$P=\begin{bmatrix}1&1&1&0&0\\1&1&1&0&0\\1&1&1&0&0\\1&1&1&1&1\\1&1&1&1&1\end{bmatrix}$.

(b) (X,Z,Y,Z).

(c) 单侧连通的.

9.38 (a) $A=\begin{bmatrix}0&7&0&0\\3&0&2&0\\0&0&0&5\\6&1&4&0\end{bmatrix}$; $Q=\begin{bmatrix}XYX&XY&XYS&XYST\\YX&YSTY&YS&YST\\STYX&STY&STYS&ST\\TX&TY&TYS&TYST\end{bmatrix}$.

9.39 (i) $A=\begin{bmatrix}0&0&0&0&1\\0&0&0&1&0\\1&1&0&1&0\\0&1&0&0&0\\1&0&1&0&0\end{bmatrix}$; $P=\begin{bmatrix}1&1&1&1&1\\0&1&0&1&0\\1&1&1&1&1\\0&1&0&1&0\\1&1&1&1&1\end{bmatrix}$.

(ii) $A=\begin{bmatrix}0&0&0&0&0&1\\1&0&1&0&0&1\\0&0&0&0&1&0\\0&1&1&0&1&0\\0&0&1&0&0&0\\0&0&0&1&0&0\end{bmatrix}$; $P=\begin{bmatrix}1&1&1&1&1&1\\1&1&1&1&1&1\\0&0&1&0&1&0\\1&1&1&1&1&1\\0&0&1&0&1&0\\1&1&1&1&1&1\end{bmatrix}$.

9.40 (i) $W=\begin{bmatrix}7&5&0&0\\0&0&0&2\\0&3&0&0\\4&0&1&0\end{bmatrix}$; $Q=\begin{bmatrix}AA&AB&ABCD&ABD\\BDA&BDCB&BDC&BD\\CBDA&CB&CBDC&CBD\\DA&DCB&DC&DCBD\end{bmatrix}$

这里 A,B,C,D 为顶点.

(ii) $W=\begin{bmatrix}0&0&1&0&5\\0&0&0&1&0\\0&0&0&4&3\\2&0&0&0&0\\0&2&0&4&0\end{bmatrix}$;

$$Q=\begin{bmatrix}ACDA&ACEB&AC&ACD&ACE\\BDA&BDACEB&BDAC&BD&BDACE\\CDA&CEB&CDAC&CD&CE\\DA&DACEB&DAC&DACD&DACEB\\EDA&EB&EDAC&ED&EDACE\end{bmatrix}$$

这里 A,B,C,D,E 为顶点.

9.41 (a) C,F,D,B,E,A. (b) $[A:C,E;\ B:D;\ C:D,E,A;\ D:A,F;\ E:\varnothing;\ F:B,E]$.

9.42 见图 9-50.

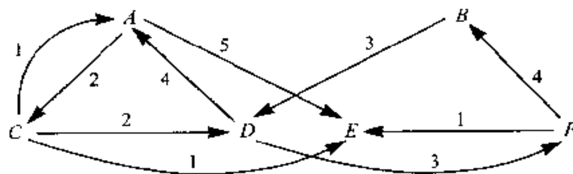


图 9-50

9.43 (a) 5,6. (b)发点 A. 收点 C. (c)见图 9-51(a). (d) 都不是.

9.44 (a) 5,6; (b) 无; (c) 见图 9-51(b); (d) 全部三个连通.

9.45 (a) 7,11; (b) 发点 A; 收点 C,D; (c) 见图 9-51(c).(d) 仅弱连通.

9.46 见图 9-52.

9.47 (a) 不存在. (b) 存在. (c) 不存在. (d) 不存在.

9.48 (a) AWP. (b) PA. (c) 不存在. (d) WPC.

9.49 $(s,4,1,2,1,2,1,2,t)$.

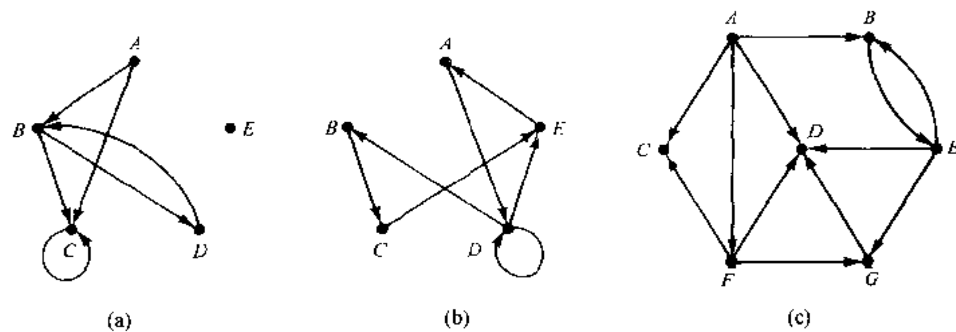


图 9－51

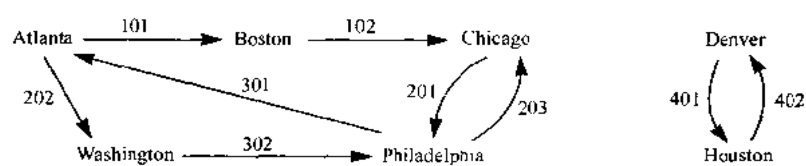


图 9－52

9.50 提示：首先画该图，(a) *ASYCZBXTD*.（b）没有，该图不是无圈的，例如，(Y,B,A,X,S,Y)是圈.（c）*ZBTYXACSDZ*.

第十章 二 叉 树

10.1 引 言

二叉树是数学与计算机科学中的基本结构.有根树的某些术语,如,边,路,枝,树叶,深度以及层次,同样用于二叉树.不过,关于二叉树,使用术语点,而不是顶点.需强调的是,二叉树不是有根树的特殊情形,它们是不同的数学对象.

10.2 二叉树

二叉树 T 定义为称为点的元素的有限集,使得

(1) T 是空的(称为空树),或

(2) T 含有一个特别的点 R,称为 T 的根,且 T 的其余点构成不交的二叉树 T_1 与 T_2 的有序对.

若 T 确有根 R,则两棵树 T_1 与 T_2 分别称为 R 的*左子树*与*右子树*.若 T_1 为非空的,则它的根称为 R 的*左后继*;类似地,若 T_2 为非空的,则它的根称为 R 的*右后继*.

上面二叉树的定义是递归的,因为 T 借助于二叉子树 T_1 与 T_2 定义.特别地,即 T 的每个点 N 含一棵左子树和一棵右子树,且或一棵或两棵子树也许是空的.因此,T 的每个点有 0,1,或 2 个后继.没有后继的点称为*终点*,于是终点的两棵子树都是空的.

二叉树的图示

二叉树常用平面上的一个示意图表示,称为 T 的*图示*,特别地,图 10-1 中的示意图表示下面的二叉树:

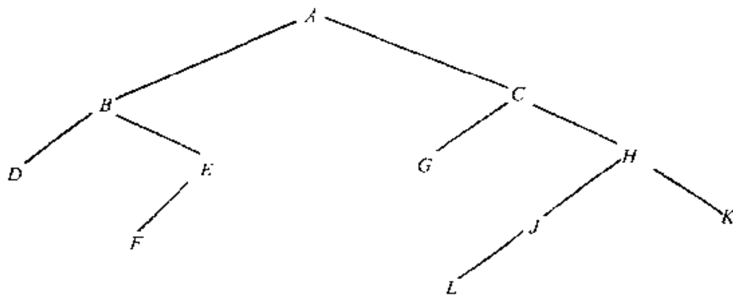


图 10-1

(i) T 有 11 个点,用字母 A~L(除 I 外)表示.

(ii) T 的根为示意图中的最高点 A.

(iii) 点 N 的左下斜线指出 N 的左后继;N 的右下斜线指出 N 的右后继.

因此,在图 10-1 中:

(a) B 为根 A 的左后继,C 为根 A 的右后继.

(b) 根 A 的左子树由点 B,D,E,F 构成;A 的右子树由点 C,G,H,J,K 与 L 构成.

(c) 点 A,B,C 和 H 都有两个后继,点 E 与 J 仅有一个后继,点 D,F,G,L 与 K 没有后继,即它们为终点.

相似二叉树

二叉树 T 与 T' 称为*相似的*,如果它们有相同的结构,或换句话说,如果它们有相同的形状.若子树称为*拷贝*.如果它们是相似的,且作为对应的点有相同的内容.

例 10.1　考虑图 10-2 中的四个二叉树，三棵树(a)，(c)与(d)是相似的，特别地，树(a)和(c)为拷贝，因为在对应的点它们有相同的数据. 树(b)既不与树(d)相似，也不是树(d)的拷贝，因为，在二叉树中，即使仅有一个后继时，也要区分左后继与右后继.

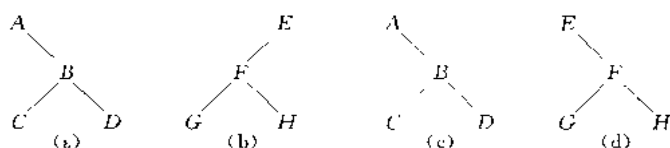


图 10-2

代数表示

考虑仅涉及二元运算的代数式 E，如

$$E=(a-b)/((c*d)+e).$$

E 可借助于图 10-3 中的二叉树 T 表示. 即 E 中的每一个二元运算作为 T 的内点，每个变量或常数作为 T 的外点，而它的左、右子树对应于该运算的运算对象. 例如，

(a) 在式 E 中，+的运算对象为 $c*d$ 与 e.

(b) 在树 T 中，点+的子树对应于子式 $c*d$ 与 e.

显然，每个代表式对应于一棵惟一的树，反之也对

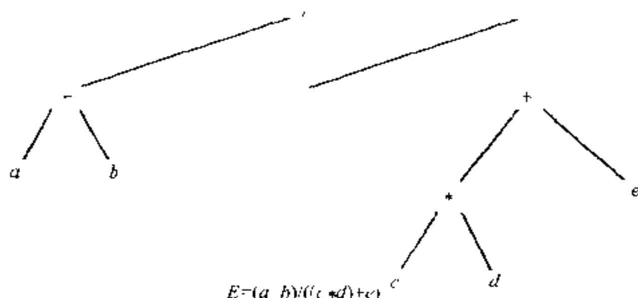


图 10-3

术语

描述家庭关系的术语常用来描述树 T 的点之间的关系. 特别地，设 N 为 T 中的点，其左后继为 S_1，右后继为 S_2，则 N 称为 S_1 和 S_2 的父母(或父亲)，类似地，S_1 称为 N 的*左孩子*(*儿子*)，S_2 称为 N 的*右孩子*(*儿子*). 进一步，S_1 与 S_2 称为*兄弟*. 二叉树 T 的每个点 N，根除外，有惟一的父母，称为 N 的前继.

术语后代与先辈有它通常的意义，即点 L 称为点 N 的*后代*(且 N 称为 L 的*先辈*)，如果存在从 N 到 L 的孩子后继. 特别地，根据 L 属于 N 的左、右子树，称 L 为 N 的*左、右后代*.

图论与园艺学的术语也用于二叉树 T. 特别地. 从 T 的点 N 到其后继的线称为*边*. 相继边的序列称为*路*，终点称为*树叶*，终于树叶的路称为*树枝*.

二叉树 T 的每个结点如下指定了一个*层次*，指定树 T 的根层次为 0，而指定其他每个点层次为比它父母层次多 1. 进一步，称有相同层次的那些点为同一代.

树 T 的*深度*(*高度*)就是 T 的树枝的最大点数，也就是比 T 的最大层次多 1. 图10-1中的树 T 的深度为 5.

10.3　完全二叉树与扩充二叉树

本节讨论两种特别的二叉树.

完全二叉树

考虑任意二叉树 T，T 的每个点至多有两个孩子. 因此，可以证明：T 的第 r 层至多有 2^r 个点. 树 T 称为完全的，若除可能最后一层外，它的所有层都有最大可能的点数，且最后一层的所有点都尽可能靠左边，于是存在惟一的恰有 n 个点的完全树 T_n（当然，不考虑结点的内容）. 图 10－4 给出了 26 个点的完全树 T_{26}.

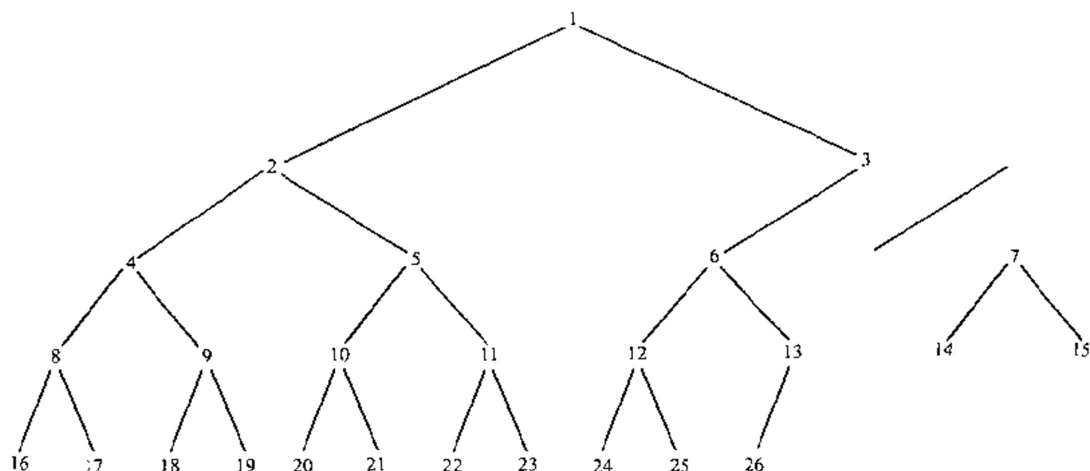


图 10－4　完全树 T_{26}

图 10－4 中完全二叉树 T_{26}的点故意一代一代地、从左到右标上整数 1，2，…，26. 利用这种标号，可以容易确定任意完全二叉树 T_n 中任一点 K 的孩子与父母. 特别地，点 K 的左、右孩子分别为 $2*K$ 与 $2*K+1$，而 K 的父母为点$\left[\frac{K}{2}\right]$. 例如，点 9 的孩子为点 18 和 19，而它的父母为点$[9/2]=4$，n 个点的完全树 T_n 的深度为

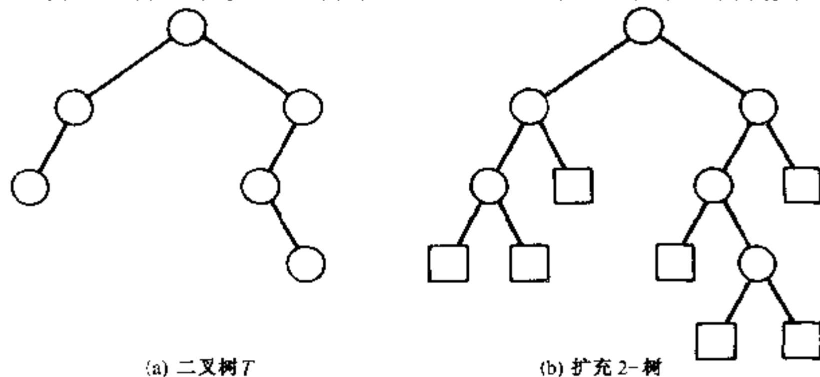
$$d_n = \lfloor \log_2 n + 1 \rfloor$$

这是一个相对小的数. 例如，若完全图 T_n 有 $n=1\ 000\ 000$ 个点，则它的深度 d_n 是 21.

扩充二叉树：2-树

二叉树 T 称为 2-树或*扩充二叉树*，如果每个点 N 或者没有孩子或有两个孩子. 如此，有两个孩子的点称为*内点*，没有孩子的点称为*外点*，有时在示意图中用圆圈代表内点，用方框代表外结点而加以区别.

术语“扩充二叉树”源于下面的运算，考虑任意二叉树 T，比如图 10－5(a)中的树，则用新点代替每个空子树就可将 T 转换为 2-树，如图 10－5(b). 注意到，新的树确实是一棵 2-树，进



(a) 二叉树 T　　　　(b) 扩充 2-树

图 10－5　将二叉树 T 转换为 2-树

一步,原来树 T 的点在扩充树中为内点,而新结点为扩充树的外点.

2-树的一个重要例子就是对应于仅有二元运算的代数式 E 的树 T,正如图 10-3 的解释,E 的变量为外点,E 的运算为内点出现.

10.4 二叉树的存贮表示

设 T 为二叉树,本节讨论存贮 T 的两种方法. 第一种,也是通常的方法,称为 T 的链表示,类似于链表的存贮方法,第二种方法用一个单组,称为 T 的序列表示. T 的表示主要要求人们应该可以直接得到 T 的根 R,且给了 T 的一 N,应该可以直接得到 N 的孩子.

二叉树的链表示

考虑二叉树 T,除非特别说明或隐含,T 用链表示存贮,即它用三个并列的组 INFO,LEFT 与 RIGHT,以及一个指针变量 ROOT 存贮. 首先,T 的每个点 N 对应了位置 K,使得

(1) INFO[K]含有点 N 的数据.

(2) LEFT[K]含有点 N 的左孩子的位置.

(3) RIGHT[K]含有点 N 的右孩子的位置.

进一步,ROOT 要含 T 的根 R 的位置. 若子树是空的,则相应的指针含有空值;若树本身是空的,则 ROOT 含空值.

注 1 多数例子将给出二叉树 T 的每个点 N 的单项信息. 在实际中,存贮了点 N 的完整记录. 换句话说,INFO 实际上也许是一个记录的线性组或并行组的集合.

注 2 空指针用 NULL 表示,且可选用任一非法地址. 实际上,用 0 或负数表示 NULL.

例 10.2 考虑图 10-1 中的二叉树 T. 图 10-6 给出了 T 的链表示的原理图. 注意到,每个点画成有三个字段,空子树用×,所有空值都用×. 图 10-7 给出了 T 的链表示在存贮中是怎样出现的,这里为方便起见写成垂直的线性组,而不是水平的线性组. 由于

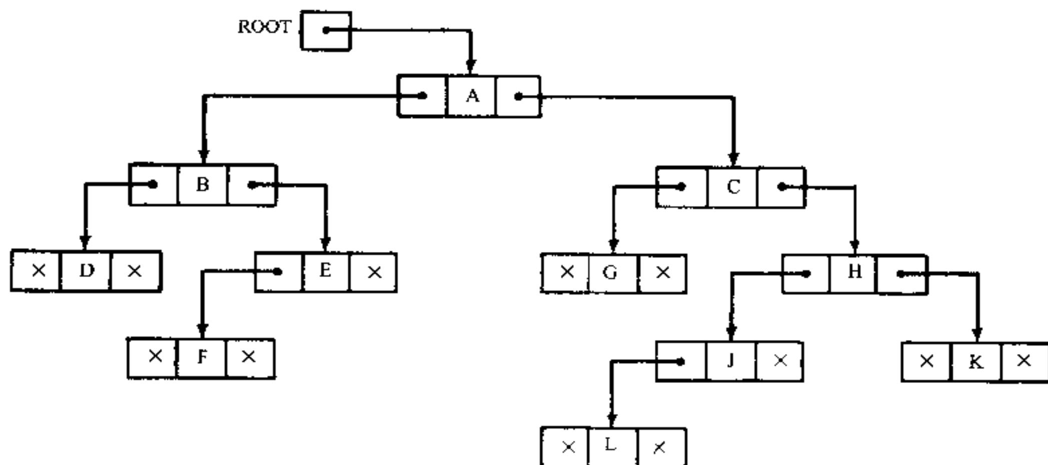


图 10-6

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
INFO	K	C	G		A	H	L			B		F	E			J	D	
LEFT	0	3	0		10	16	0			17		0	12			7	0	
RIGHT	0	6	0		2	1	0			13		0	0			0	0	

ROOT 5

图 10-7

A 为 T 的根，所以 ROOT$=5$ 指向 INFO[5]$=A$，又由于 B 为 A 的左孩子，所以 LEFT[5]$=10$ 指向 INFO[10]$=B$，且由于 C 为 A 的右孩子，所以 RIGHT[5]$=2$ 指向 INFO[2]$=C$. 组中 18 个元素的选取是任意的.

二叉树的序列表示

设 T 是完全或几乎完全的二叉树，则有一个有效的方法存贮 T，称为 T 的序列表示，这种表示只用一个单线性组 TREE 以及指针变量 END，使得

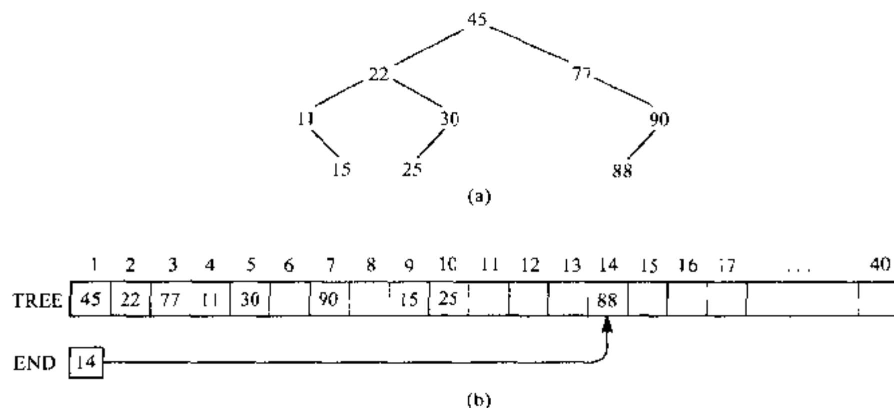
(a) T 的根 R 存贮在 TREE[1]中.

(b) 若点 N 占据 TREE[K]，则它的左孩子存贮在 TREE[$2*K$]中，而它的右孩子存贮在 TREE[$2*K+1$]中.

(c) END 包含 T 的最后点的位置.

进一步，根据 $2*K$ 或 $2*K+1$ 是否超过 END，或根据 TREE[$2*K$]或 TREE[$2*K+1$]是否含空值，确定在 TREE[K]的点 N 是否有空左、右子树.

图 10-8(a)中的二叉树 T 的序列表示如图 10-8(b). 注意到尽管 T 只有 9 个点，但组 TREE 需要 14 个位置. 一般来说，深度 d 的树的序列表示将需要大致 2^d 个元素的组，因此，这种序列表示通常是低效的，除非如上所述，二叉树 T 是完全的或几乎完全的. 例如，图 10-1 中的树 T 有 11 个结点，深度为 5，意味着可能需要大致 $2^5=32$ 个元素的组.



(a)

(b)

图 10-8

10.5 穿过二叉树

有三种标准的方法穿过根为 R 的二叉树 T，这三种算法分别称为前序的、内序的和后序的.

前序 (1) 处理根 R.

(2) 依前序穿过 R 的左子树.

(3) 依前序穿过 R 的右子树.

内序 (1) 内序穿过 R 的左子树.

(2) 处理根 R.

(3) 内序穿过 R 的右子树.

后序 (1) 依后序穿过 R 的左子树.

(2) 依后序穿过 R 的右子树.

(3) 处理根 R.

注意到每个算法含有同样的三步，且 R 的左子树总在右子树前穿过，算法之间的差别就是处理根 R 的时间，特别地，在"前序"算法中，根 R 在穿过子树之前处理在"内序"算法中，根 R 在穿过两子树之间处理；而在"后序"算法中，根 R 在穿过子树之后处理.

这三个算法有时也分别称为点左右(NLR)法、左点右(LNR)法、左右点(LRN)……

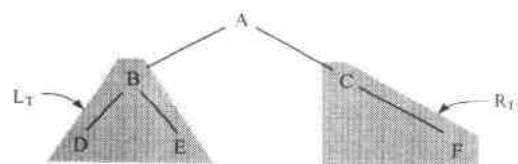


图 10－9

有平均运行时间 $f(n)=O(\log_2 n)$ 的元素，这里 n 为数据项的个数，也能让我们容易地插入与删除元素. 与下面的结构对比：

(a) *排序线性组*　能查找和求具有平均运行时间 $f(n)=O(\log_2 n)$ 的元素，然而插入和删除元素是费事的，因为平均要移动 $O(n)$ 个元素.

(b) *链表*　可容易地插入和删除元素. 但是，查找和求一个元素是费事的，因为必须用运行时间为 $f(n)=O(n)$ 的线性查找.

尽管二叉查找树中的每个点也许含数据的完整记录，但树的定义依赖于给定的字段，该字段的值是不同的，且也许是有序的.

定义　设 T 为二叉树，如果 T 的每个点有下面的性质：

N 的值大于 N 的左子树中的每个值，小于 N 的右子树中的每个值.

则 T 称为*二叉查找树*.

不难看出上面的性质保证了 T 的内序截给出 T 的元素的排序列表.

注　上面二叉查找树的定义假设所有点的值不同，有一个类似的二叉查找树 T 的定义，它允许重复，即每个点有下面的性质：

(a) 对 N 的左子树中的每个点 M，$N>M$.

(b) 对 N 的右子树中的每个点 M，$N\leqslant M$.

当采用这个定义时，下面讨论的运算必须作相应地修改.

例 10.5　图 10－11(a) 中的二叉树是二叉查找树，即 T 的每个点 N 超过它的左子树中的每个数，小于它的右子树的每个数，若用 35 替换 23，则 T 仍是二叉查找树. 另一方面，若用 40 替换 23，则 T 不再是二叉查找树. 因为 40 在 38 的左子树中，但 $40>38$.

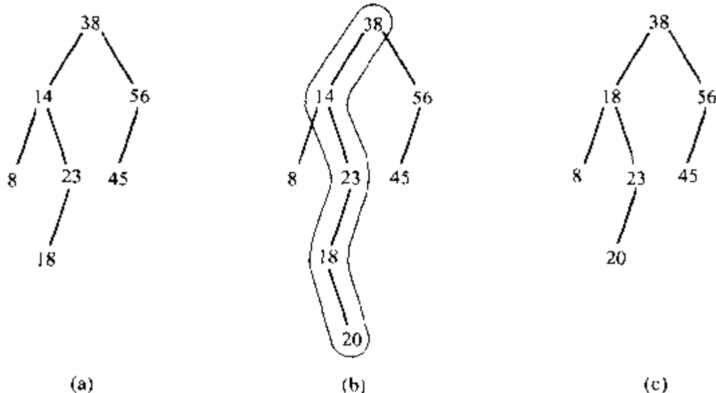


图 10－11

(a) 在二叉查找树中查找与插入：下面是在二叉查找树中的查找与插入算法.

> **算法 10.6A**　已知二叉查找树 T 和信息项 ITEM，该算法求 T 中 ITEM 的位置，或在 ITEM 中插入树的新点.
>
> **Step 1**　与树的根 N 比较 ITEM.
>
> (a) 若 ITEM$<N$，则处理 N 的左孩子.
>
> (b) 若 ITEM$>N$，则处理 N 的右孩子.
>
> **Step 2**　重复 Step 1，直至下列之一发生.
>
> (a) 找到 N 使得 ITEM$=N$. 如此，查找成功.
>
> (b) 找到空子树，说明查找不成功，在这个空子树的位置插入 ITEM.
>
> **Step 3**　退出.

例 10.6 考虑图 10 - 11(a)中的二叉查找树 T,已知 ITEM=20,要查找或插入 ITEM 到 T、模仿算法 10.6A 可得下面的步骤.

(1) 将 ITEM=20 与根 $R=38$ 比较,因为 $20<38$,所以,处理 38 的左孩子,是 14.

(2) 将 ITEM=20 与 14 比较,因 $20>14$,故处理 14 的右孩子,是 23.

(3) 将 ITEM=20 与 23 比较,因 $20<23$,故处理 23 的左孩子,是 18.

(4) 将 ITEM=20 与 18 比较,因 $20>18$,而 18 没有右孩子,作为 18 的右孩子插入 20.

图 10 - 11(b)给出了 ITEM=20 插入后的新树且算法中沿树的路被圈起来.

(b) 二叉查找树的删除法:下面的算法从二叉查找树中删除给定的 ITEM.它用算法 10.6A 查找 ITEM 在 T 中的位置.

算法 10.6B 已知二叉查找树 T 和信息项 ITEM,$P(N)$表示点 N 的父母,$S(N)$表示点 N 的内序后继,该算法从 T 中删除 ITEM.

Step 1 用算法 10.6A 查找含 ITEM 的点 N 的位置,并保留父母点 $P(N)$的位置轨迹.(若 ITEM 不在 T 中,则停止,并退出.)

Step 2 确定 N 的孩子数,有三种情形:

(a) N 没有孩子.从 T 中删去 N,并在父母点 $P(N)$处用 NULL 指针简单地替换 N 的位置.

(b) N 恰有一个孩子 M.从 T 中删去 N,并在父母点 $P(N)$处用 M 的位置代替 N 的位置.(用 M 取代 N).

(c) N 有两个孩子.

(i) 求 N 的内序后继 $S(N)$(则 $S(N)$没有左孩子).

(ii) 用(a)或(b)在 T 中删去 $S(N)$.

(iii) 在 T 中用 $S(N)$取代 N.

Step 3 退出.

注 注意到 Step 2 (c)中的情形(iii)比前两种情形更复杂.如下找到 N 的内序后继.从点 N 向右移到 N 的右孩子,再逐步地向左,直到找到没有左孩子的结点 M,点 M 为 N 的内序后继 $S(N)$.

例 10.7 考虑图 10 - 11(b)中的二叉树 T,从 T 中删去 ITEM=14.首先找点 N,使 $N=14$.注意到 N 有两个孩子,移向右,再左,求得 N 的内序后继 $S(N)=18$.删去 $S(N)=18$,并用它仅有的孩子 20 代替.再用 $S(N)=18$ 代替 $N=14$.得到图 10 - 11(c)中的树.

二叉查找树算法的复杂性

设二叉树 T 有 n 个结点,且深度为 d,令 $f(n)$表示上面任一算法的运行时间.算法 10.6A 从根 R 开始持续经过树 T,直至在 T 中找到 ITEM 或作为终点插入 ITEM.算法 10.6B 从根 R 开始持续经过树 T,先找 ITEM,再继续在树 T 上找 ITEM 的内序后继.无论什么情形,移动的次数不超过树的深度 d,因此,任一算法的运行时间依赖于树 T 的深度 d.

现设 T 有性质:对 T 的每个点 N,N 的子树的深度至多差 1.那么,树 T 称为平衡的,且 $d\sim\log_2 n$.于是,平衡树的任一算法的运行时间 $f(n)$是很快的.特别地,$f(n)=O(\log_2 n)$.另一方面,当在二叉查找树 T 中添加新点,并没有保证 T 依然平衡,甚至会发生 $d\sim n$.此时,$f(n)$变得相当地慢,特别地,$f(n)=O(n)$,幸运的是,在 T 中添加元素时,有技术使得二叉查找树 T 再平衡.不过,这种技术已超出本书的范围.

10.7　优先队列，堆积

设 S 为优先队列，即 S 为一个集合，其元素定时地插入与删除，但总是删除当前最大的元素(具有最高优先性的元素)，可如下存贮 S：

(a) **线性组**　只需在该组的末尾添加一个元素就容易地插入了这个元素. 然而，查找与求最大元素却是费事的，因为这需用运行时间 $f(n)=O(n)$的一个线性查找.

(b) **排序线性组**　最大元素或是第一个，或是最后一个，因此，删除它是容易的. 然而，插入和删除元素却是费事的，因为平均需要移动 $O(n)$个元素.

本节介绍一个离散结构，它能有效地实施优先队列 S.

堆积

设 H 为 n 个元素的完全二叉树，并设 H 用它的序列表示，而不是链表示存贮.(见§10.4)

定义　设 H 为完全二叉树，若 H 中的每个点 N 有下面的性质：

N 的值大于或等于 N 的每个孩子的值.

则 H 称为堆积或大堆积.

因此，堆积中 N 的值超过它的每个后代的值，特别地，H 的根是 H 的最大值.

小堆积可类似的定义：N 的值小于或等于它的每个孩子的值.

例 10.8　考虑图 10-12(a)中的完全二叉树，注意到 H 是堆积. 特别地，是指 H 的最大元素出现在堆积的"顶". 图 10-12(b)用组 TREE 和变量 END 给出了 H 的序列表示. 因此，

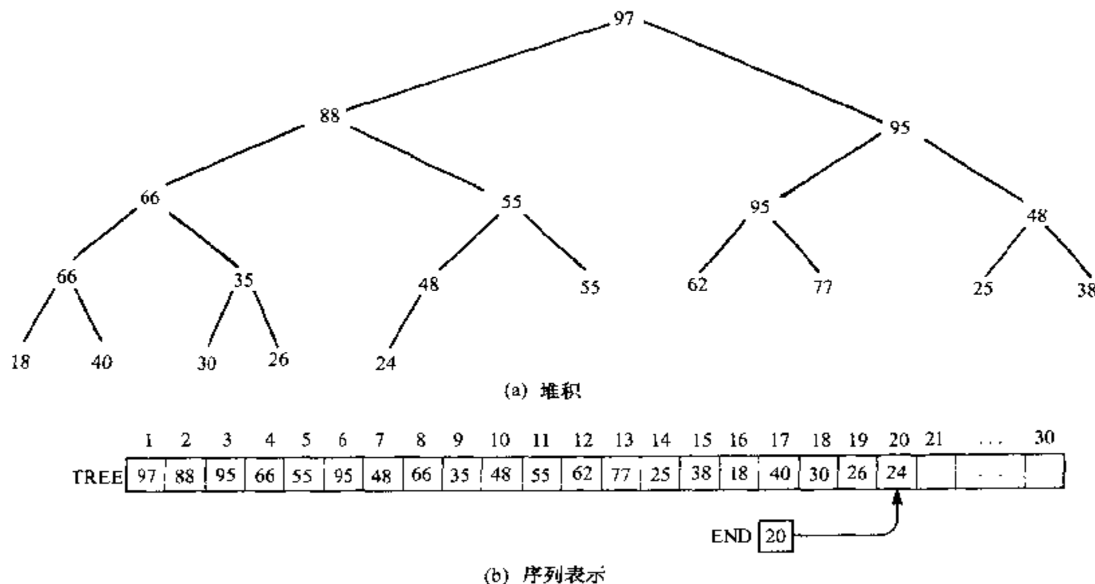


图 10-12

(a) TREE[1]为 H 的根 R.

(b) TREE[$2k$]与 TREE[$2k+1$]为 TREE[k]的左、右孩子.

(c) 变量 END=20 指向 H 的最后元素.

(d) 任意非根点 TREE[j]的父母是点 TREE[$J\div 2$](这里 $J\div 2$ 指取整除法.)

注意到 H 的同一层次的点在组 TREE 中一个接一个地出现：TREE 的 30 个位置的选择是任意的.

(a) **堆积中插入**　下面的算法对堆积 H 插入给定的信息项 ITEM.

算法 10.7A 已知堆积 H 与新的 ITEM,该算法在 H 中插入 ITEM.

Step 1 在 H 的尾部联 ITEM,使得 H 仍为完全树,但不必为堆积.

Step 2(再堆积) 设在 H 中将 ITEM 提升到"适当的位置",使得 H 为堆积,即

(a) 将 ITEM 与它的父母 P(ITEM)比较,若 ITEM>P(ITEM),则互换 ITEM 与 P(ITEM).

(b) 重复(a)直至 ITEM≤P(ITEM)

Step 3 退出.

注 必须证明,作为最后的树,上面的算法总给出一个堆积.这点不难看出,其证明留给读者.

例 10.9 考虑图 10-12 中的堆积 H,假设在 H 中插入 ITEM=70.模仿算法 10.7A,首先作为完全树的最后元素联 ITEM:即,置 TREE[21]=70,且 END=21.然后重新堆积,即如下将 ITEM 上升到适当位置:

(a) 将 ITEM=70 与其父母 48 比较,因 70>48,故互换 70 和 48.

(b) 将 ITEM=70 与其新父母 55 比较,因 70>55,故互换 70 和 55.

(c) 将 ITEM=70 与其父母 88 比较,因 70<88,故 ITEM=70 已上升到 H 的适当位置.

图 10-13 给出了插入 ITEM=70 后的最后的树,由 ITEM 沿树向上的路被圈起来.

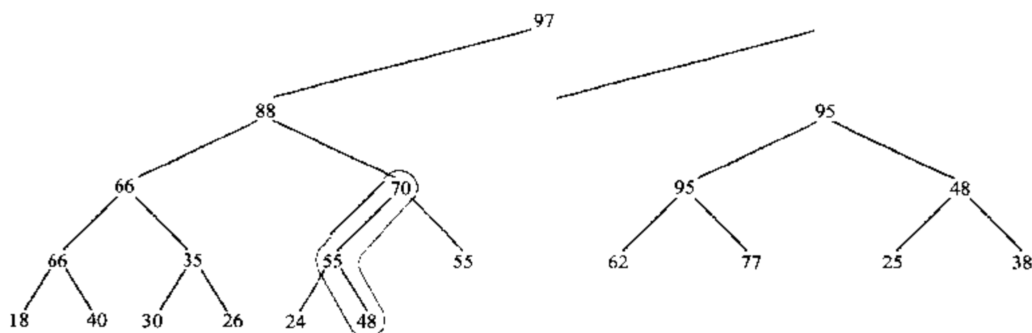


图 10-13 插入 ITEM=70

(b) **从堆积中删除根** 下面的算法从一个堆积 H 中删除根 R.

算法 10.7B 该算法从给定的堆积 H 中删除根 R.

Step 1 指定根 R 到某个变量 ITEM.

Step 2 用 H 中的最后点 L 取代删去的根 R,使得 H 仍为完全二叉树,但不必是堆积.[即,置 TREE[1]:=TREE[END],再置 END:=END−1.]

Step 3(重新堆积) 让 L 在 H 中下沉到"适当位置",使得 H 是堆积,即:

(a) 求 L 的较大的孩子 LARGE(L).若 L<LARGE(L),则互换 L 与 LARGE(L).

(b) 重复(a)直至 L≥LARGE(L).

Step 4 退出.

注 与在堆积中插入一样,也必须证明上面的算法总给出一个堆积作为最后的树.仍将这个证明留给读者.还注意到,也许 Step 3 在点 L 到达树的底,即 L 没有孩子时才结束.

例 10.10 考虑图 10-14(a)中的堆积 H.这里 R=95 是根,L=22 是 H 的最后,要从堆积 H

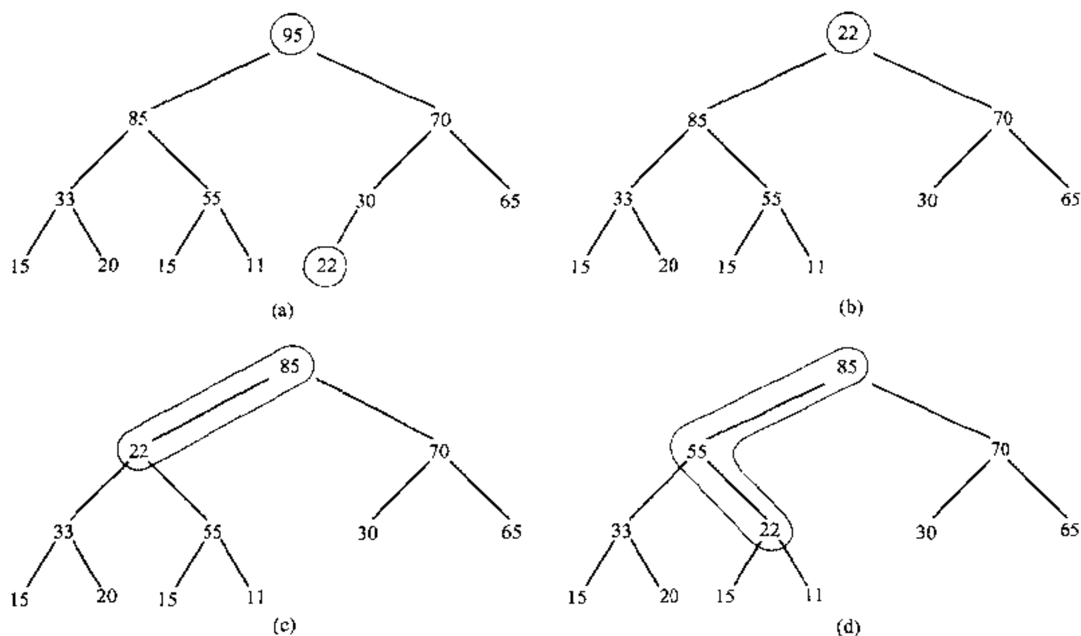


图 10-14

中删除 $R=95$. 模仿算法 10.7B，首先指定 ITEM=95，再用 $L=22$ 代替 $R=95$，这就给出图 10-14(b) 中的完全树，它不是堆积.（注意到 22 的两个子树仍都是堆积.）然后重新堆积，即令 $L=22$ 如下下沉到适当位置.

(a) $L=22$ 的孩子为 85 和 70，较大者为 85，因 $22<85$，故互换 22 和 85，即为图 10-14(c) 中的树.

(b) $L=22$ 的孩子现为 33 和 55，较大者为 55. 因 $22<55$，故互换 22 和 55，即为图 10-14(d) 中的树.

(c) $L=22$ 的孩子现为 15 和 11，较大者为 15，因 $22\geqslant15$，故点 $L=22$ 已下沉到堆积中的适当位置.

因此，图 10-14(d) 为所需的堆积 H，没有了原来的根 $R=95$. 注意到图中圈住了 $L=22$ 沿树下沉的路.

堆积算法的复杂性

设 H 为 n 个点的堆积，因 H 为完全树，故 $d\approx\log_2 n$，这里 d 为 H 的深度. 由算法 10.7A 可知新的 ITEM 沿着树一层一层地向上处理，直到在 H 中找到它的适当位置. 由算法 10.7B 可知，原来的最后点 L 沿着树一层一层地向下处理，直到在 H 中找到它的适当位置. 无论如何，移动的次数都不会超过 H 的深度 d. 于是两种算法的运行时间 $f(n)$ 都是非常快的，特别地，$f(n)=O(\log_2 n)$. 因此，堆积是实施优先队列 S 的有效方法，它比本节开头提到的线性组或排序线性组更有效得多.

10.8 路长，Huffman 算法

设 T 为扩充 2 叉树或 2-树（§10.3）. 即 T 为每个点 N 或没有孩子或有两个孩子的二叉树，没有孩子的点称为外点，而有两个孩子的点称为内点，有时为了在示意图中区别这些点，用圆圈表示内点，用方框表示外点. 此外，若 T 有 n 个外点，则 T 有 $n-1$ 个内点. 图 10-15 给出了有 7 个外点，从而有 $7-1=6$ 个内点的 2-树.

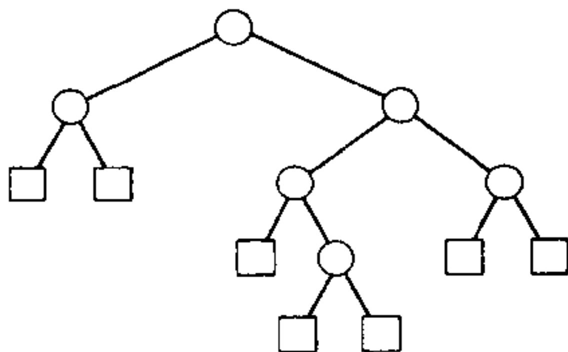


图 10 - 15

赋权路长

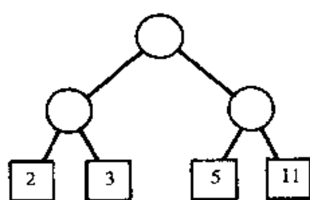
设 T 为 n 个外点的 2-树，且给每个外点指定一个（非负）权，树 T 的**赋权路长**（简称**路长**）P 定义为和

$$P = W_1L_1 + W_2L_2 + \cdots + W_nL_n,$$

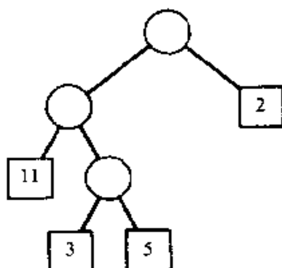
这里 W_i 为外点 N_i 的权，L_i 为从根 R 到点 N_i 的路长.（即使对未赋权的 2-树，路长 P 也存在，因为只要假设每个外点的权为 1.）

例 10.11 图 10 - 16 中给出了三个 2-树 T_1, T_2 和 T_3，每个 2-树外点的权都是 2,3,5 和 11，这三个 2-树的赋权路长如下：

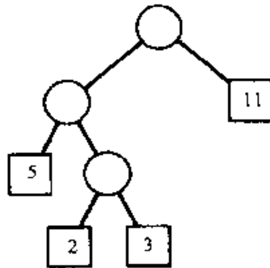
$$P_1 = 2(2) + 3(2) + 5(2) + 11(2) = 42,$$
$$P_2 = 2(1) + 3(3) + 5(3) + 11(2) = 48,$$
$$P_3 = 2(3) + 3(3) + 5(2) + 11(1) = 36.$$



(a) T_1.



(b) T_2.



(c) T_3.

图 10 - 16

数 P_1 与 P_2 表明完全树未必给出最小的路长，而数 P_2 与 P_3 表明相类似的树也未必给出相同的路长.

Huffman 算法

我们要解决的一般问题如下：设已知 n 个权的列表，比如

$$w_1, w_2, \cdots, w_n$$

在带有 n 个给定权的 n 个外点的所有 2-树中，求具有最少赋权路长的树 T.（这样的树很少惟一.）Huffman 给出了求这种树 T 的一个算法.

下面的 Huffman 算法利用权的个数 n 递归地定义. 实际上，使用 Huffman 算法的等价的迭代形式，它是从下往上而不是从上往下地构造了所需的树 T.

算法 10.8（Huffman） 该算法递归地求具有 n 个给定权 $w_1, w_2, \cdots, w_n$，且有最小赋权路长的赋权 2-树 T.

Step 1 若 $n=1$，则令 T 为有一个结权为 w_1 的点 N 的树，然后退出.

Step 2 若 $n>1$，

(a) 在 n 个给定的权中，求两个最小权，设为 w_i 和 w_j.

(b) 求树 T'，使得对这 $n-1$ 个权，T' 为最小赋权路长的树.

(c) 在树 T' 中，用子树（根为 ○，左子 $\boxed{w_i}$，右子 $\boxed{w_j}$）代替外点 $\boxed{w_i+w_j}$.

(d) 退出.

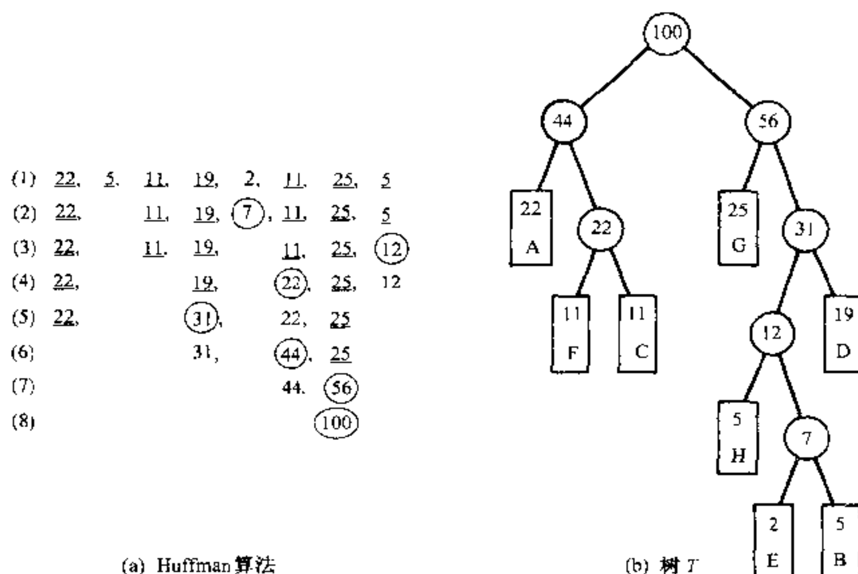
例 10.12 设 A,B,C,D,E,F,G,H 是八个具有下面指定权的数据项.

数据项：	A	B	C	D	E	F	G	H
权：	22	5	11	19	2	11	25	5

构造一棵 2-树 T，使 T 的外点具有上面的数据且 T 具有最小赋权路长 P.

应用 Huffman 算法，即重复地将两个最小权的子树联为一个单子树，如图10－17(a). 为清楚起见，原来的权带有下划线，而圈内数表示新子树的根. 从 Step(8) 返回画出树 T，见图 10－17(b).（当分裂一个点为两个部分时，就在左边画出更小的点.）路长 P 如下：

$$P = 22(2)+11(3)+11(3)+25(2)+5(4)+2(5)+5(5)+19(3) = 272.$$



(a) Huffman算法 (b) 树 T

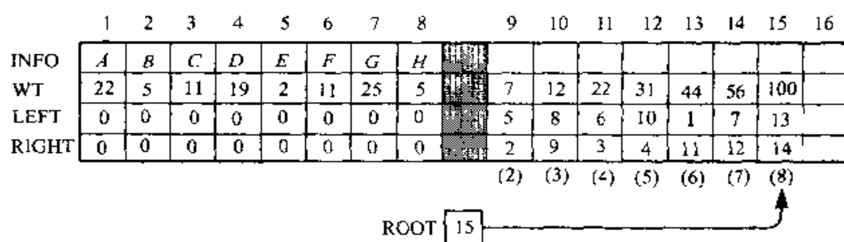
图 10－17

Huffman 算法的计算机实现

再考虑例 10.12 中的数据，假设要利用计算机实现这个算法. 由于二叉树中的某些点是赋权的，所以该树可用四个平行组：INFO，WT，LEFT 与 RIGHT 存贮. 图 10－18 中的前八列表示数据最初在计算机中是如何存贮的.

Huffmas 算法的每一步给从第 9 至第 15 列的 WT，LEFT 与 RIGHT 指定数值. 它们分别对应了图 10－17 中的第(2)至第(8)步. 特别地，每一步求出当前的两个极小权及它们的位置，然后和进入 WT，且它们的位置进入 LEFT 与 RIGHT. 例如，在给第 11 列（对应于 step(4)）指

定数值后，当前的极小权是 12 和 19，出现在 WT[10]与 WT[4]中. 因此，指定 WT[12]=12+19=31，且 LEFT[12]=10，RIGHT[12]=4. 由最后一步知，ROOT=15，或利用 ROOT=$2n-1$，而外点的数目 $n=8$. 因此，整个图 10－18 给出所求的树 T.



	1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16
INFO	A	B	C	D	E	F	G	H									
WT	22	5	11	19	2	11	25	5		7	12	22	31	44	56	100	
LEFT	0	0	0	0	0	0	0	0		5	8	6	10	1	7	13	
RIGHT	0	0	0	0	0	0	0	0		2	9	3	4	11	12	14	
										(2)	(3)	(4)	(5)	(6)	(7)	(8)	

图 10－18

注　在执行 Huffman 算法时，需保留当前权的情况，并求两个最小的权、这可用保持一个辅助小堆积有效地完成，这个小堆积的每个点含一个权以及它在树中的位置、之所以用小堆积而不用大堆积是因为要使最小权的点位于堆积的顶.

编码应用

假设一组 n 个数据项 $A_1,A_2,\cdots,A_n$ 要用位的串来编码，这样做的一个方法是用 r 位串来编码每个项，而 $n<2^r$. 例如，48 个字符的集合可用 6-位串来编码存贮，但不能用 5-位串编码存贮，因为 $2^5=32<48$.

如果数据项并不以相同的概率发生，那么用变长的字符串可节约存贮的空间与时间，此时，频繁出现的项用较短的字符串，不常出现的项用较长的字符串. 例如，国家电话编码就使用这个原则，美国的国家电话编码就是 1，法国为 33，芬兰为 358. 本节讨论变长编码，这个基于赋权数据项的 Huffman 树，即具有最小路长 P 的 2-树 T.

Huffman 码　设 n 个数据项 $A_1,A_2,\cdots,A_n$ 被赋权，且 T 为这些数据的 Huffman 树，T 的每条边依据其指向左孩子还是右孩子而赋值 0 或 1. Huffman 码将从树 T 的根 R 到外点 A_i 的位序列指派给 A_i.

上述 Huffman 码有前缀性质，即每个项的码都不是任何其他项的码的开始的子串，这就是说，用 Huffman 码解码任何信息时不会有任何混乱.

例 10.13　再考虑例 10－12 中的八个数据项 A,B,C,D,E,F,G,H，假设权代表数据项发生的百分数概率. 给图 10－17(b)中的 Huffman 树的每条边指定位标号，得到图 10－19的树 T. 读者可以验证树 T 给出下面的码：

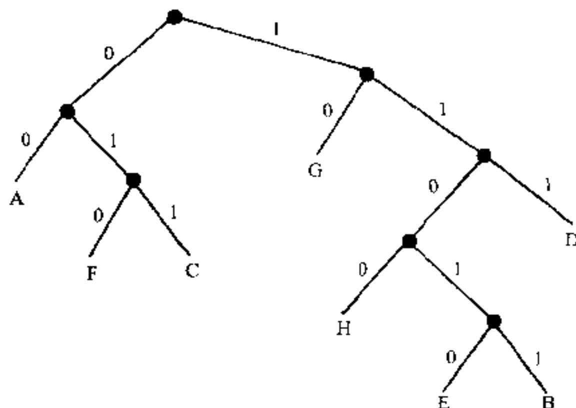


图 10－19

A:00,　B:11011,　C:011,　D:111,
E:11010,　F:010,　G:10,　H:1100.

这是这些数据项的有效编码.

10.9　一般(有序有根)树回顾

设 T 为有序根树(§9.4),也称为一般树,T 可正式地定义为称为点的元素的非空集合,使得:

(1) T 含有一个可区别出的元素 R,称为 T 的根.

(2) T 的其余元素构成 0 或更多不交树 $T_1,T_2,\cdots,T_m$ 的有序集合簇.

称树 $T_1,T_2,\cdots,T_m$ 为根 R 的子树,而 $T_1,T_2,\cdots,T_m$ 的根称为 R 的后继.

与二叉树一样,对一般的树也使用家庭关系、图论以及园艺学中的术语,特别地,若 N 是有后继 $S_1,S_2,\cdots,S_m$ 的点,则 N 称为这些 S_i 的父母,而 S_i 称为 N 的孩子,这些 S_i 之间相互称为兄弟.

例 10.14　图 10-20 给出了 13 个点的一般树 T 的示意图,这 13 个点为 $A,B,C,D,E,F,G,H,J,K,L,M,N$.

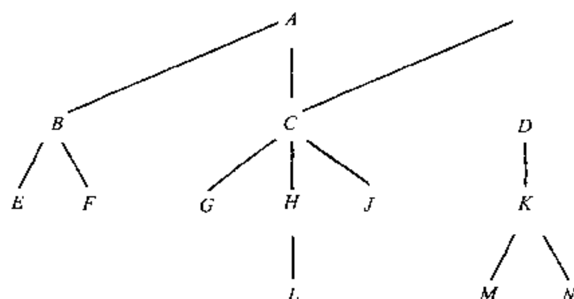


图 10-20

除非说明,树 T 的根为示意图顶上的结点,且每个点的孩子从左到右排序. 因此 A 为 T 的根,且 A 有三个孩子,第一个孩子为 B,第二个为 C,第三个为 D. 注意到:

(a) 点 C 有三个孩子.

(b) 点 B 和 K 都有两个孩子.

(c) 点 D 和 H 都仅有一个孩子.

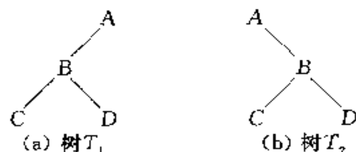
(d) 点 E,F,G,L,J,M,N 没有孩子.

最后一组点没有孩子,称为终点.

注　二叉树 T' 并不是一般树 T 的特例. 它们是两个不同的对象,两个主要区别如下:

(1) 二叉树 T' 可以是空的,但一般树 T 不空.

(2) 若点 N 仅有一个孩子,则在二叉树 T' 中,这个孩子是左孩子还是右孩子是不同的,但在一般树 T 中没有这种差别.



(a) 树 T_1　(b) 树 T_2

图 10-21

在图 10-21 中用树 T_1 和 T_2 解释了第二种区别. 特别地,作为二叉树,T_1 与 T_2 是不同的树,因为在树 T_1 中,B 为 A 的左孩子,而在树 T_2 中,B 为 A 的右孩子,另一方面,作为一般树,树 T_1 与 T_2 之间没有区别.

森林

森林 F 定义为 0 或多个不同树的有序簇,显然,若删去一般树 T 的根 R,则得到由 R 的子树(也许是空的)构成的森林 F. 反过来,若 F 为一个森林,则连一个点 R 到 F 就构成一个一般树 T,这里 R 为 T 的根,R 的子树由 F 中的原来的树构成.

一般树的计算机表示

设 T 为一般树，除非特别说明或隐含，T 用下面的链表示存贮，这个链表示用三个平行组 INFO，CHILD(或 DOWN)，与 SIBL(或 HORZ)，以及一个指针变量 ROOT. 首先，T 的每个点 N 对应了一位置 K，使得：

(1) INFO[K]含点 N 的数据.

(2) CHILD[K]含 N 的第一个孩子的位置，当 CHILD[K]=NULL 时，表明 N 没有孩子.

(3) SIBL[K]含有 N 的下一个兄弟的位置，当 SIBL[K]=NULL 时，表明 N 是它父母的最后一个孩子.

进一步，ROOT 含有 T 的根 R 的位置，尽管这种表示看起来是人工的，但它有重要的优点，即 T 的每个点 N，无论 N 有多少孩子，N 都恰含有三个字段.

上面的表示容易被推广到表示森林 F，F 含有子树 $T_1, T_2, \cdots, T_m$，只要假设这些子树的根是兄弟. 此时，ROOT 含有第一棵树 T_1 的根 R_1 的位置，否则 F 为空的，ROOT=NULL.

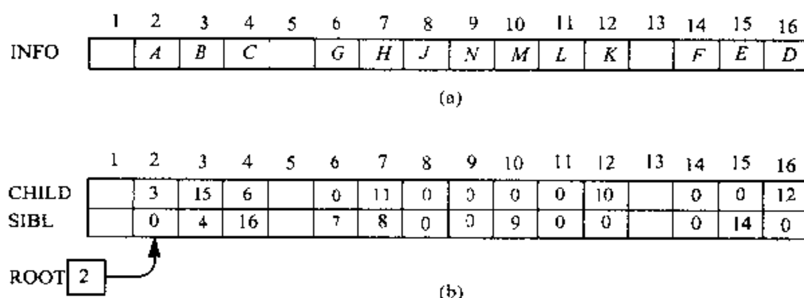
例 10.15 考虑图 10-20 中的一般树 T，设 T 的点的数据存贮在图 10-22(a)的组 INFO 中，如下给指针 ROOT 和组 CHILD 与 SIBL 指定值就得到 T 的构造亲缘关系：

(a) 因 T 的根 A 存贮在 INFO[2]中，故置 ROOT:=2.

(b) 因 A 的第一个孩子为点 B，它存在 INFO[3]中，故置 CHILD[2]:=3. 又 A 没有兄弟姊妹，故置 SIBL[2]:=NULL.

(c) 因点 B 的第一个孩子是点 E 存在 INFO[15]中，故置 CHILD[3]:=15. 又点 C 为 B 的下一个兄弟，且 C 存在 INFO[4]中，故置 SIBL[3]:=4.

等等，图 10-22(b)给出了 CHILD 与 SIBL 的最后的值.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
INFO		A	B	C		G	H	J	N	M	L	K		F	E	D

(a)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CHILD		3	15	6		0	11	0	0	0	0	10		0	0	12
SIBL		0	4	16		7	8	0	0	9	0	0		0	14	0

ROOT 2

(b)

图 10-22

一般树与二叉树间的对应

设 T 为一般树，则对 T 可以如下指定惟一的二叉树 T'. 首先，二叉树 T'的点与一般树 T 的结点完全相同，而 T'的根仍为 T 的根. 设 N 为二叉树 T'的任一点，则 N 在 T'中的左孩子为结点 N 在一般树 T 中的第一个孩子，T'中 N 的右孩子为一般树 T 中 N 的下一个兄弟.

一般树 T 的计算机表示与相应的二叉树 T'的链表示恰好是相同的，只是一般树 T 中的组名 CHILD 和 SIBL 对应于二叉树 T'中的组名 LEFT 和 RIGHT. 这种对应的重要性在于适用于二叉树的某些算法，比如截算法，也可以适用于一般树.

例 10.16 考虑图 10-20 中的一般树 T，读者能够验证图 10-23 中的二叉树 T'对应于一般树 T. 注意到，逆时针旋转图 10-23 中的 T'的示意图，直至指向右孩子的边成水平方向，就得到各点与图 10-20 的点有相同的相对位置的图. 进一步，二叉树 T'的计算机表示可以在图 10-22 中的一般树 T 的计算机表示中将 CHILD 换为 LEFT，将 SIBL 换为 RIGHT 得到.

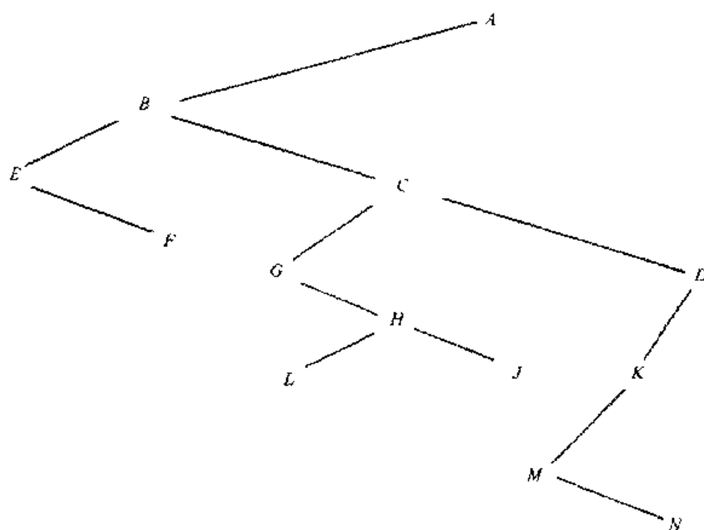


图 10-23　二叉树 T'

问题与解答

二叉树

10.1　设二叉树 T 如图 10-24 存贮，画出 T 的示意图.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
INFO	20	30	40	50	60	70	80	90			35	45	55	95
LEFT	0	1	0	0	2	0	0	7			0	3	11	0
RIGHT	0	13	0	0	6	8	0	14			12	4	0	0

ROOT 5

图 10-24

解　从树 T 的根开始，如下画出 T.

(a) 从指针 ROOT 的值得到根 R，注意到 ROOT=5，因此，INFO(5)=60 为 T 的根 R.

(b) 从 R 的左指针字段得到 R 的左孩子，注意到 LEFT[5]=2，因此 INFO[2]=30为 R 的左孩子.

(c) 从 R 的右指针字段得到 R 的右孩子，注意到 RIGHT[5]=6，因此，INFO[6]=70为 R 的右孩子.

现可以画出该树的顶部，如图 10-25(a)，对每个新的点重复上面的过程，最后得到如图 10-25(b)中

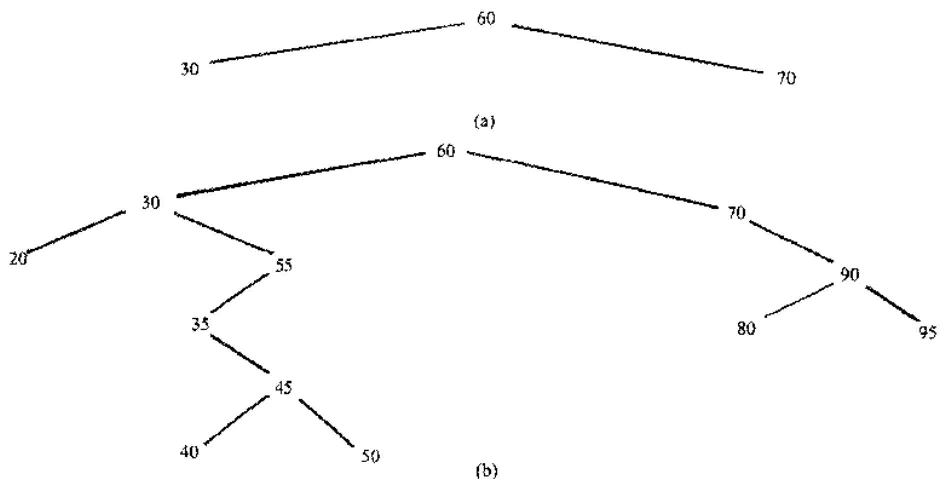


图 10-25

所需的树.

10.2 考虑图 10-26 中的三棵树 T_1, T_2, T_3，指出哪些表示相同的(a) 根树，(b) 有序根树，(c) 二叉树？

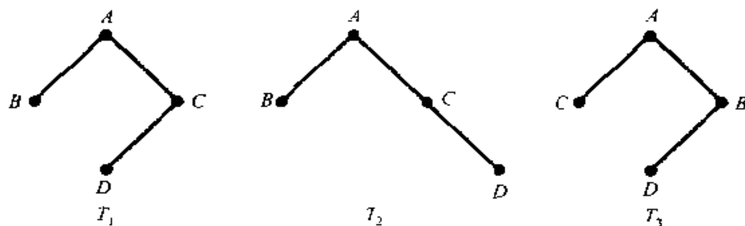


图 10-26

解 (a) 它们都表示相同的根树. 即 A 是根有孩子(直接后继)B 和 C，且 C 有单个孩子 D.

(b) T_1 与 T_2 为相同的有序根树，但 T_3 不是，特别地，在 T_1 与 T_2 中 B 为 A 的第一个孩子，但在 T_3 中 B 为 A 的第二个孩子.

(c) 它们代表不同的二叉树，特别地，T_1 与 T_2 不同，因为即便是只有一个后继也要区分左、右后继(对有序根树不真)，即 T_1 中 D 为 C 的左后继，T_2 中 D 为 C 的右后继.

10.3 考虑图 10-27 中的二叉树 T，求存贮中 T 的序列表示.

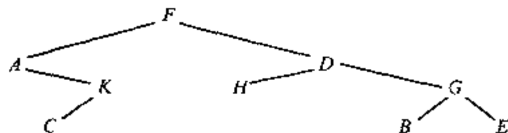


图 10-27

解 T 的序列表示只用单线性组 TREE 与变量指针 END.

(a) T 的根 R 存贮在 TREE[1]中，因此 TREE[1]$=F$.

(b) 若点 N 在 TREE[K]，则它的左、右孩子分别存贮在 TREE[$2*K$]与 TREE[$2*K+1$]中. 因此 TREE[2]$=A$，TREE[3]$=D$，因为 A 与 D 为 F 的左、右孩子，等等. 图 10-28 包含了 T 的序列表示，注意到 TREE[10]$=C$. 因为 C 为 K 的左孩子，而 K 存贮在 TREE[5]，也有 TREE[14]$=B$，TREE[15]$=E$，因为 B 和 E 为 G 的左，右孩子，G 存贮在 TREE[7].

(c) END 指向 T 的最后一点的位置，因此 END$=15$.

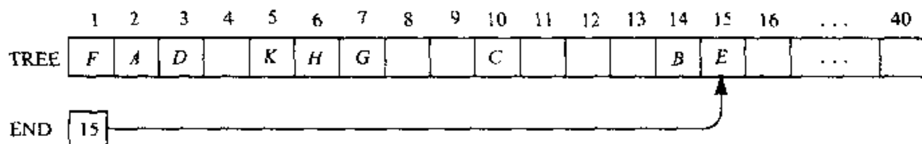


图 10-28

10.4 考虑图 10-27 中的二叉树 T.

(a) 求 T 的深度 d，d 与 T 的序列表示如何相关.

(b) 用前序算法穿 T.

(c) 用内序算法穿 T.

(d) 用后序算法穿 T.

(e) 求 T 的终点以及在(b)，(c)，(d)中穿过的序.

解 (a) 深度 d 为 T 的最长树枝中的点数，因此 $d=4$.(注意到 END 总位于 2^d 与 2^{d+1} 之间. 特别地，$2^d \leqslant \text{END} < 2^{d+1}$. 正如所料，$8 \leqslant \text{END} < 16$.)

(b) T 的前序截为递归的 NLR 算法. 即首先过点 N，然后它的左子树 L，最后它的右子树 R，用[A_1，A_2，…，A_k]表示点为 $A_1, A_2, \cdots, A_k$ 的子树，则树 T 如下穿过：

$$F-[A,K,C][D,H,G,B,E] \text{ 或 } F-A-[K,C]-D-[H][G,B,E]$$

或最后为

$$F-A-K-C-D-H-G-B-E.$$

(c) T 的内序截为递归的 LNR 算法，即先左子树 L，再点 N，最后右子树 R，于是 T 如下通过.

$$[A,K,C]-F-[D,H,G,B,E] \text{ 或 } A-[K,C]-F-[H]-D-[G,B,E]$$

或最后为

$$A-C-K-F-H-D-B-G-E.$$

(d) T 的后序截为递归的 LRN 算法，即先左子树 L，再右子树 R，最后点 N，于是 T 如下通过

$$[A,K,C][D,H,G,B,E]-F \text{ 或}[K,C]-A-[H][G,B,E]-D-F$$

或最后为

$$C-K-A-H-B-E-G-D-F.$$

(e) 终点是没有孩子的点，在所有三个截算法中以相同的次序通过：C,H,B,E.

10.5 二叉树 T 有 9 个结点，若 T 的前序截与内序截给出下面的结点序列：

前序：$G\quad B\quad Q\quad A\quad C\quad P\quad D\quad E\quad R.$

内序：$Q\quad B\quad C\quad A\quad G\quad P\quad E\quad D\quad R.$

画出 T 的示意图.

解 ☞　由根向下如下画出树 T.

(a) 选择前序中的第一点得到 T 的根，因此 G 为 T 的根.

(b) 点 G 的左孩子如下得到，先用 T 的内序求 G 的左子树 T_1 中的点. 因此 T_1 由 Q,B,C,A 构成，在 T 的内序中，它们在 G 的左边，然后在 T_1 的前序(即以 T 的前序出现)中选第一点(根)就得到 G 的左孩子，因此 B 为 G 的左孩子.

(c) 类似地，G 的右子树由点 P,E,D,R 构成，且 P 为 T_2 的根，即 P 为 G 的右孩子.

对每个新点重复上面的过程，最后得到图 10 - 29 中所需的树.

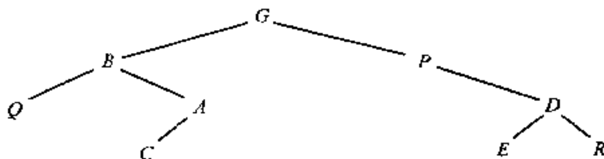


图 10 - 29

10.6 考虑代数式 $E=(2x+y)(5a-b)^3$.

(a) 画出对应于式 E 的树 T.

(b) 求指数运算的范围，即，求以指数运算为根的子树.

(c) 求 T 的前序.

解 ☞　(a) 用箭头(↑)表示指数，星号(＊)表示乘法，得到图 10 - 30 中的树.

(b) ↑的范围为图 10 - 30 中阴影部分的子树，它对应于子式$(5a-b)^3$.

(c) 从左开始扫描该树(如图 10 - 10 中)得到

$$* + * 2xy \uparrow - * 5ab3$$

(这恰好为代数式 E 的前缀波兰符号.)

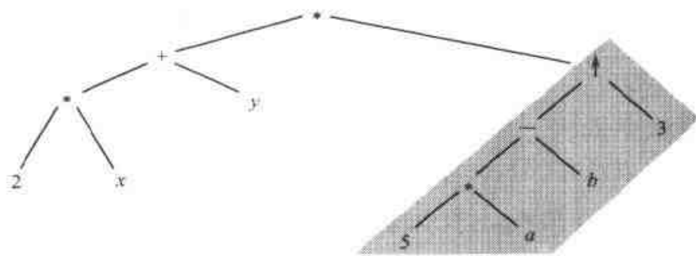


图 10 - 30

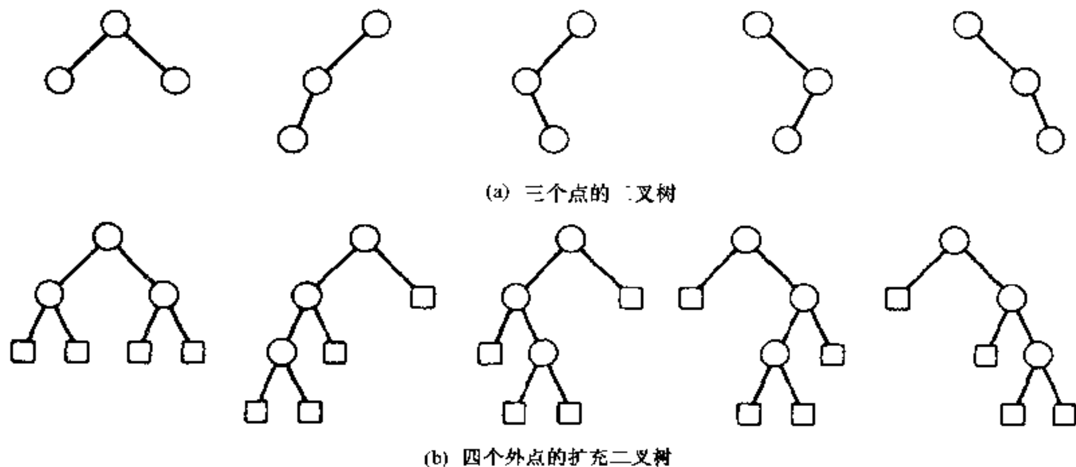
10.7 画出所有可能的不相似的树 T，这里

(a) T 是三个点的二叉树.

(b) T 是四个外点的 2-树.

解 ☞ (a) 有五个这样的树,如图 10-31(a).

(b) 四个外点的每个 2-树由三个点的二叉树确定,即由(a)中的树确定.因此有五个这样的树,如图 10-31(b).



(a) 三个点的二叉树

(b) 四个外点的扩充二叉树

图 10-31

二叉查找树,堆积

10.8 考虑图 10-25(b)中的二叉树 T.

(a) T 为什么是二叉查找树?

(b) 若 ITEM=33 加到树中,求新树 T.

解 ☞ (a) 由于每个点 N 大于它的左子树的值,小于它的右子树的值,因此 T 为二叉查找树.

(b) 与根 60 比较 ITEM=33,因为 33<60,故移到左孩子 30;因为 33>30,故移到右孩子 55,又因为 33<55,故移到左孩子 35,由于 33<35,且 35 没有左孩子.因此,添加 ITEM=33 作为结点 35 的左孩子就给出图 10-32 中的树,阴影的边指出了插入过程中沿树向下的路.

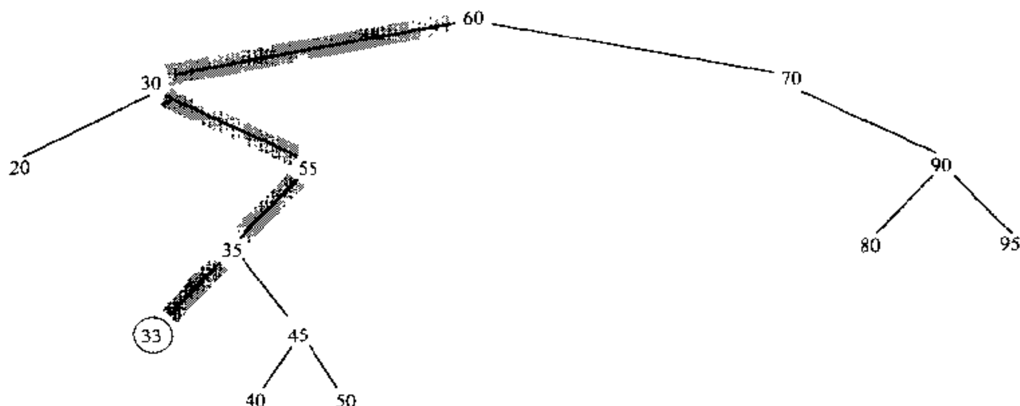


图 10-32

10.9 将下面的字母列表插入到空的二叉查找树中.

$$J,R,D,G,W,E,M,H,P,A,F,Q.$$

(a) 求最后的树 T.　(b) 求 T 的内序截.

解 ☞ (a) 一个接一个插入点便得到图 10-33 中的树 T.

(b) T 的内序截如下:

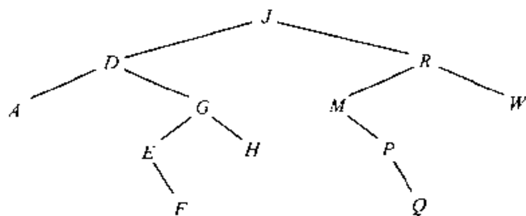


图 10－33

$$A,D,E,F,G,H,J,M,P,Q,R,W.$$

注意到这是字母的字母序列表.[任何二叉查找树 T 的内序截给出点的排序列表.]

10.10 考虑图 10－33 中的二叉查找树 T. 描述(a) 删除点 M，且(b) 删除点 D 后的树 T.

解 ☞ (a) 点 M 仅有一个孩子 P，因此，删去 M，且令 P 为 R 的左孩子而取代 M.

(b) 点 D 有两个孩子，求 D 的内点后继为 E. 首先从树中删去 E，再用点 E 取代 D.

图 10－34 给出了更改后的树 T.

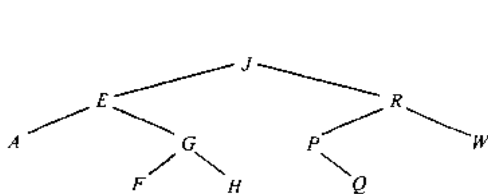


图 10－34

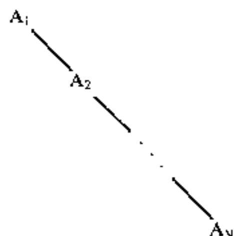


图 10－35

10.11 设 n 个数据项 $A_1,A_2,\cdots,A_N$ 已排序，即 $A_1<A_2<\cdots<A_N$.

(a) 若各项依次插入到空二叉树 T，描述最后的树 T.

(b) 求最后的树 T 的深度 d.

(c) 对(i) $n=50$，(ii) $n=100$，(iii) $n=500$，将 d 与 n 个点的二叉树的平均深度 d^* 比较.

解 ☞ (a) 树 T 由向右延伸的一树枝构成，如图 10－35.

(b) T 的树枝有 n 个点，因此，$d=n$.

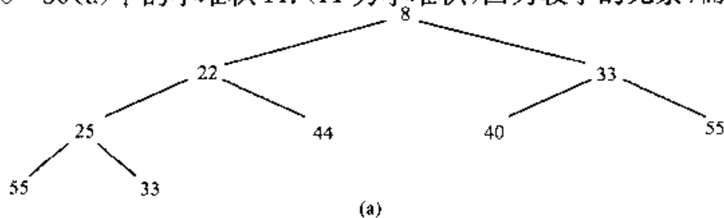
(c) 已知 $d^*=c\log_2 n$，这里 $c\approx1.4$. 故

(i) $d(50)=50$;　$d^*(50)\approx9$.

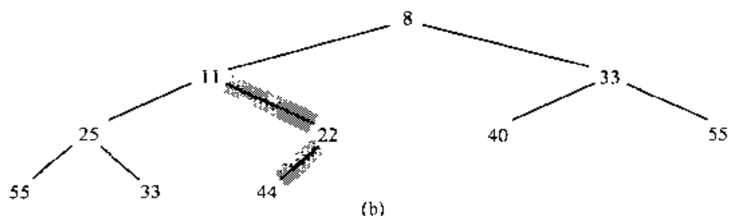
(ii) $d(100)=100$;　$d^*(100)\approx10$.

(iii) $d(500)=500$;　$d^*(500)\approx12$.

10.12 考虑图 10－36(a)中的小堆积 H.（H 为小堆积，因为较小的元素，而不是较大的元素，



(a)



(b)

图 10－36

在堆积的顶.)描述将 ITEM=11 插入到 H 后的堆积.

解☞ 首先,作为完全树中的下一点插入 ITEM,即作为点 44 的左孩子插入,则重复地比较ITEM与它的 PARENT(父母),并且只要 ITEM<PARENT 就交换 ITEM 与 PARENT. 因为 11<44,交换 11 和 44,因 11<22,交换 11 和 22.因11>8,ITEM=11 已找到在堆积 H 中适当的位置,图 10-36(b)给出了最后的堆积 H,阴影的边表示 ITEM 沿树向上的路.

10.13 考虑图 10-37 中 $N=6$ 个点的完全树 T,并设 T 以组 A 序列地存贮,对 $J=1,2,\cdots,N-1$,反复地插入 $A[J+1]$到堆积 $A[1]$到 $A[J]$,从 T 构成堆积 H.(如问题 10.12)

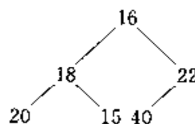


图 10-37

解☞ 图 10-38 给出了各步骤,现分别解释每一步.

(a) $J=1$ 且 ITEM=$A[2]$=18,因 18>16,故交换 18 和 16.

(b) $J=2$ 且 ITEM=$A[3]$=22,因 22>18,故交换 22 和 18.

(c) $J=3$ 且 ITEM=$A[4]$=20,因 20>16,但 20<22,只交换 20 和 16.

(d) $J=4$,且 ITEM[5]=15,因 15<20,故没有发生交换.

(e) $J=5$ 且 ITEM[6]=40,因 40>18,40>22,故先交换 40 和 18,再交换 40 和 22.

现在的树是堆积,点划线表明发生的交换.未涂阴影的区域表明树构成堆积的部分,注意到堆积由上往下得到(尽管每个元素沿树往上移动).

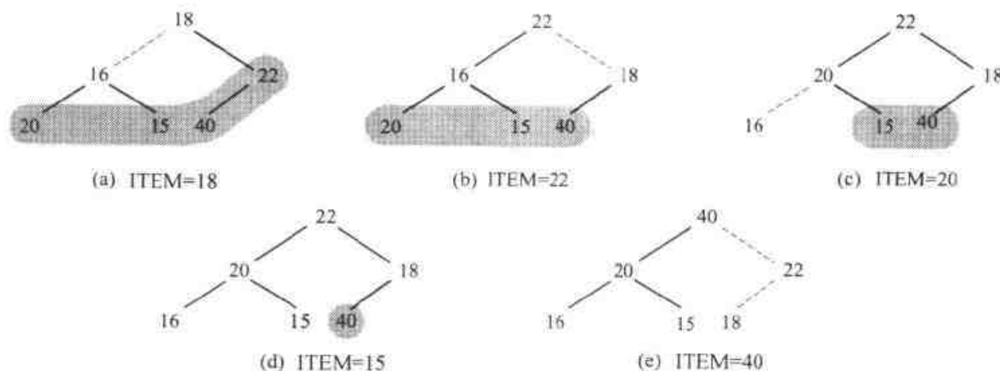


图 10-38

路长,Huffman 算法

10.14 考虑图 10-39 中的赋权 2-树,求树 T 的赋权路长 P.

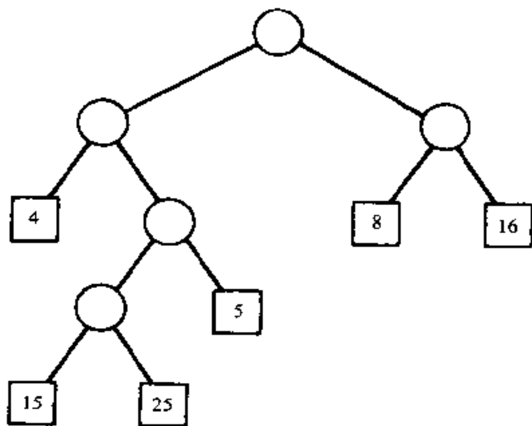


图 10-39

解☞ 用权 W_i 乘以从 T 的根到含有该权的点的路的长度 L_i,然后再相加这些乘积便得到 P,因此:

$$P = 4(2) + 15(4) + 25(4) + 5(3) + 8(2) + 16(2)$$
$$= 8 + 60 + 100 + 15 + 16 + 32 - 231.$$

10.15 设已知六个权 4,15,25,5,8,16,求有给定权及最小路长 P 的 2-树.(将 T 与图 10-39 中的树比较.)

解 ☞ 利用 Huffman 算法,即如下反复地将两个最小权的子树连成单个子树:

(a) 4, 15, 25, 5, 8, 16　(d) 25, 17, (31)

(b) 15, 25, (9), 8, 16　(e) (42) 31

(c) 15, 25, (17) 16　(f) (73)

(圆圈中的数表明在各步中新树的根.)从 Step(f)返回画出 T,给出图 10-40,由树 T 计算得:

$$P = 25(2) + 4(4) + 5(4) + 8(3) + 15(2) + 16(2)$$
$$= 50 - 16 + 20 + 24 + 30 + 32 = 172.$$

(图 10-39 中的树路长为 231.)

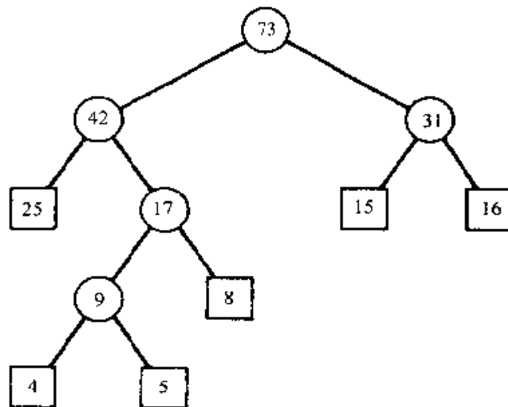


图 10-40

10.16 假设数据项 A,B,C,D,E,F,G 以下面的概率分布出现:

数据项:A　B　C　D　E　F　G.
概　率:10　30　5　15　20　15　5.

求该数据的 Huffman 码.

解 ☞ 用 Huffman 算法如下求具有最小权路长 P 的 2-树 T:

(a) 10, 30, 5, 15, 20, 15, 5

(b) 10, 30, (10) 15, 20, 15

(c) (20), 30, 15, 20, 15

(d) 20 30, (30) 20

(e) (40), 30, 30

(f) 40 (60)

(g) (100)

(圆圈中的数还是表示各步中新子树的根.)从 Step(g)返回,给出了图 10-41. 对树 T 的树枝指定位标号,左枝为 0,右枝为 1. 如图 10-41,树 T 给出下面的 Huffman 码.

A: 000　B: 11　C: 0010　D: 100　E: 01　F: 101　G: 0011.

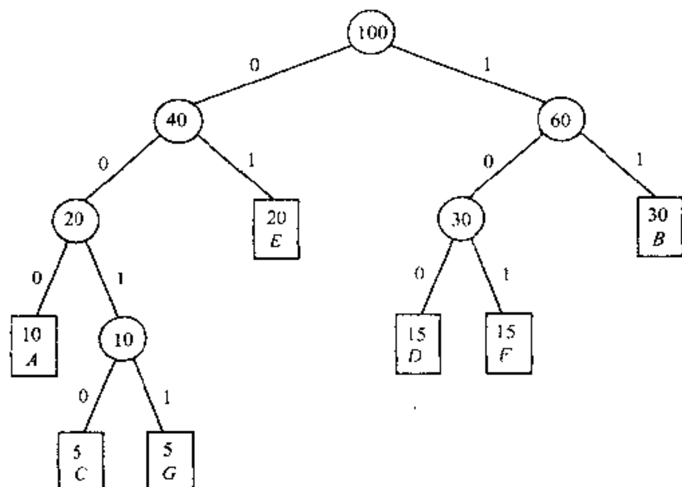


图 10－41

一般树

10.17　考虑图 10－42(a)中的一般树 T,求相应的二叉树 T'.

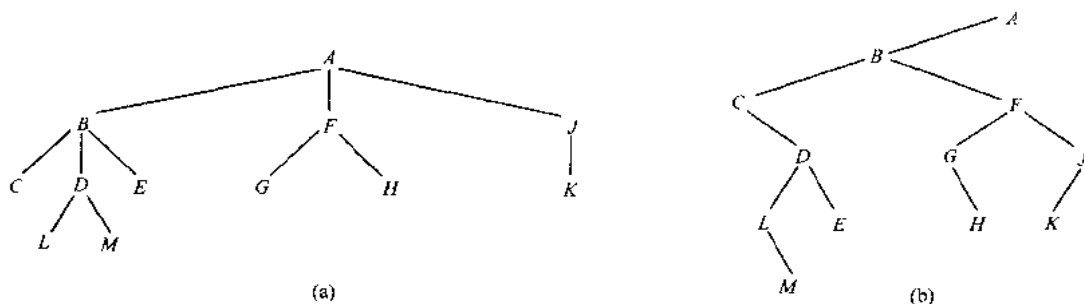


图 10－42

解 ☞　T'的点与一般树 T 的点完全一样,且特别地,T'的根也是 T 的根.进一步,若 N 为二叉树 T'的点.则它的左孩子是 N 在 T 中的第一个孩子,而它的右孩子即为 T 中 N 的下一个兄弟.由根往下构造 T',得到图 10－42(b)中的树.

10.18　设一般树 T 的根为 R,子树为 $T_1, T_2, \cdots, T_M$,T 的前序截与后序截如下定义:

前序:　(1) 处理根 R.

　　　(2) 以前序方式穿过子树 $T_1, T_2, \cdots, T_M$.

后序:　(1) 以后序方式穿过子树 $T_1, T_2, \cdots, T_M$.

　　　(2) 处理根 R.

设 T 为图 10－42(a)中的一般树,按(a) 前序,(b) 后序穿过 T.

解 ☞　注意到 T 有根 A 及子树 T_1, T_2, T_3,使得

T_1 由结点 B,C,D,E,L,M 构成.

T_2 由结点 F,G,H 构成.

T_3 由结点 J,K 构成.

(a) T 的前序截由以下几步构成:

(i) 处理根 A.

(ii) 以前序截 T_1:处理结点 B,C,D,L,M,E.

(iii) 以前序截 T_2:处理结点 F,G,H.

(iv) 以前序截 T_3:处理结点 J,K.

因此,T 的前序截如下:

$$A,B,C,D,L,M,E,F,G,H,J,K.$$

(b) T 的后序截由下列几步构成：

(i) 以后序截 T_1：处理结点 C,L,M,D,E,B.

(ii) 以后序截 T_2：处理结点 G,H,F.

(iii) 以后序截 T_3：处理结点 K,J.

(iv) 处理根 A.

因此，T 的后序截如下：

$$C,L,M,D,E,B,G,H,F,K,J,A.$$

10.19 考虑图 10－42(b)中的二叉树 T'，求 T' 的前序截，内序截与后序截. 将这些截与图 10－42(a)中对应的一般树 T 的前序截与后序截（问题 10.18 中得到的截）进行比较.

解 ☞ 利用§10.5 中二叉树截算法，得到 T' 的下面的截：

前序：$A,B,C,D,L,M,E,F,G,H,J,K.$

内序：$C,L,M,D,E,B,G,H,F,K,L,A.$

后序：$M,L,E,D,C,H,G,K,J,F,B,A.$

注意到二叉树 T' 的前序与一般树 T 的前序一致，且二叉树 T' 的内序截与一般树 T 的后序截一致，但没有一般树 T 的自然截对应于相应的二叉树的后序截.

补　充　题

二叉树

10.20 考虑图 10－43(a)中的二叉树 T.

(a) 求(i) T 的深度 d；(ii) B 的后代.

(b) 以(i) 前序，(ii) 内序，(iii) 后序列出 T 的点.

10.21 考虑图 10－43(a)中的二叉树 T.

(a) 求存贮 T 时的链表示，假设 T 的点用下面 10 个位置存贮在线性组 INFO 中：

INFO[1]$=A$,　INFO[2]$=C$,　INFO[3]$=E$,　INFO[4]$=G$,

INFO[7]$=B$,　INFO[8]$=D$,　INFO[9]$=F$,　INFO[10]$=H$.

(b) 求存贮 T 时的序列表示.

10.22 对图 10－43(b)中的二叉树 T 重复问题 10.20 与 10.21.

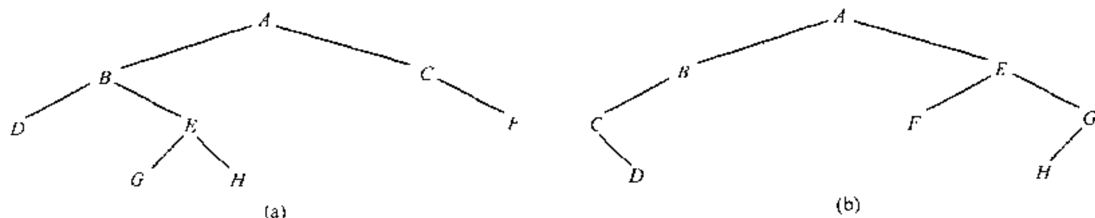


图 10－43

10.23 设二叉树 T 如图 10－44 存贮，而 ROOT＝14.

(a) 画出 T 的示意图.

(b) 以(i) 前序，(ii) 内序，(iii)后序列出 T 的点.

(c) 求 T 的深度 d. 若 T 以 TREE 序列地存贮，求线性组 TREE 所需位置的最小数.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
INFO	H	R		P	B		E		C	F	Q	S		A	K	L		D
LEFT	4	0		0	18		1		0	15	0	0		5	2	0		0
RIGHT	11	0		0	7		0		10	15	12	0		9	0	0		0

图 10－44

10.24　设二叉树 T 的前序截与内序截给出下面的点序列.

前序：　$G,B,Q,A,C,K,F,P,D,E,R,H.$

内序：　$Q,B,K,C,F,A,G,P,E,D,H,R.$

(a) 画出 T 的示意图.

(b) 求(i) T 的深度 d；(ii) B 的后代.

(c) 列出 T 的终点.

10.25　画出对应于代数式 $E=(x+3y)^4(a-2b)$ 的 2-树 T，并求 T 的前序.

二叉查找树，堆积

10.26　设下面的数插入到空的二叉查找树 T 中，画出最后的树 T：

50，　33，　44，　22，　77，　35，　60，　40.

10.27　考虑图 10－45 中的二叉查找树 T.若点 20，55 和 88 一个接一个地加到 T 中，求最后的树 T.

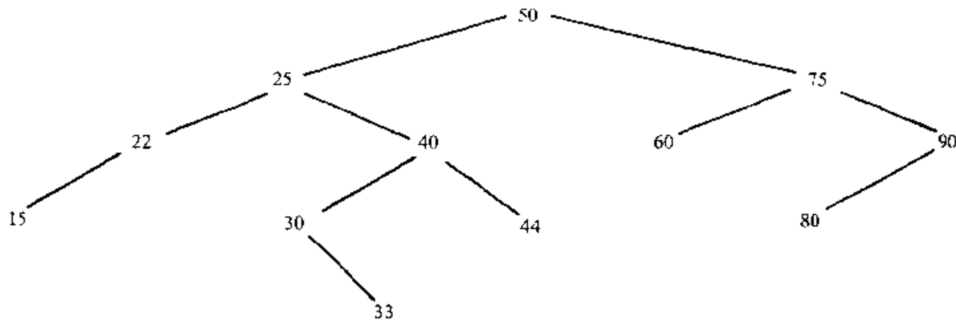


图 10－45

10.28　考虑图 10－45 中的二叉查找树 T.若点 22，25 和 75 一个接一个地从 T 中删除，求最后的树 T.

10.29　考虑图 10－46 中的 $N=10$ 个点的完全树 T.

(a) 求用组 A 存贮 T 的序列表示.

(b) 通过反复地插入 $A[J+1]$ 到堆积 $A[1]$ 到 $A[J]$（如问题 10.13 所做），从 T 构造大堆积 H.

(c) 从 T 构造小堆积 H'（取代大堆积）.

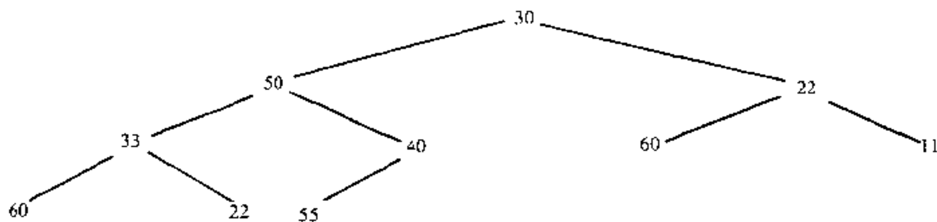


图 10－46

Huffman 算法，一般树

10.30　考虑图 10－47 中的 2-树 T，它有七个字母 A,B,C,D,E,F,G 作为外点.求由树 T 确定的字母的 Huffman 编码.

10.31　设给七个数据项 $A,B,\cdots,G$ 指定下面的权：

$(A,13)$，　$(B,2)$，　$(C,19)$，　$(D,23)$，　$(E,29)$，　$(F,5)$，　$(G,9)$.

求图 10－47 中树的赋权路长 P.

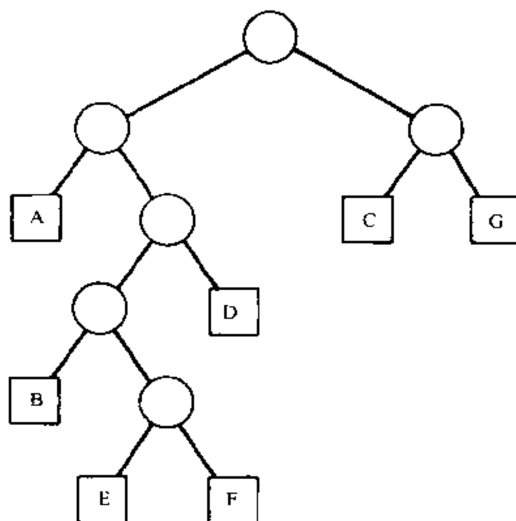


图 10-47

10.32 利用问题 10.31 中的数据，用有最小赋权路长 P 的 2-树，求这七个字母的 Huffman 编码，并求 P.

10.33 考虑图 10-48 中的森林 F，它有根分别为 A,B,C 的三棵树，画出对应于 F 的二叉树 F'.

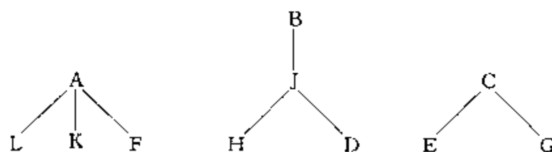


图 10-48

计算机问题

问题 10.34～10.39 参照图 10-49，它是存贮的雇员记录列表，相关于 NAME，它是二叉查找树. 也用一个领导点列出 SSN[HEAD]中的雇员数以及 SALARY[HEAD]中的全部工资. 同样，为允许插入，可用(空)的位置构成了 AVAIL 的链表，其指向列表中的第一个元素，且链表用组 LEFT 存贮.

HEAD: 5

AVAIL: 8

	NAME	SSN	SEX	SALARY	LEFT	RIGHT
1					0	
2	Davis	192-38-7282	女	22 800	5	12
3	Kelly	165-64-3351	男	19 000	5	5
4	Green	175-56-2251	男	27 200	2	5
5		009		191 600	14	5
6	Brown	178-52-1065	女	14 700	5	5
7	Lewis	181-58-9939	女	16 400	3	10
8					11	
9	Cohen	177-44-4557	男	19 000	6	4
10	Rubin	135-46-6262	女	15 500	5	5
11					13	
12	Evans	168-56-8113	男	34 200	5	5
13					1	
14	Harris	208-56-1654	女	22 800	9	7

图 10-49

10.34 编制程序按字母序打印雇员记录列表.（提示：以内序打印记录.）

10.35 编制程序读取雇员的名字 NNN，并打印出该雇员的记录，用(a) Evans，(b) Smith，(c) Lewis 检测程序.

10.36 编制程序读取雇员的社会保险号 SSN，并打印出该雇员的记录. 用(a) 165-64-3351，(b) 135-46-

6262,(c)177-44-5555 检测程序.

10.37 编制程序读取整数 K,且当 $K=1$ 时打印出每个男雇员的姓名;当 $K=2$ 时打印出每个女雇员的姓名.用(a) $K=2$,(b) $K=5$,(c) $K=1$ 检测程序.

10.38 编制程序读取雇员的姓名 NNN,并从结构中删除该雇员的记录,用(a) Davis,(b) Jones,(c) Rubin 检测程序.

10.39 编制程序读取新雇员的记录,且将记录插入到文件,用(a) Fletcher;168-52-3388;女;21000. (b) Nelson;175-32-2468;男;19000 检测程序.

补充题答案

10.20 (a) (i) $d=4$;(ii) D,E,G,H.

(b) (i) $ABDEGHCF$;(ii) $DBGEHACF$;(iii) $DGHEBFCA$.

10.21 见(a) 图 10-50(a);(b) 图 10-51(a),而 END=11.

10.22 (a) (i) $d=4$;(ii) C,D.

(b) (i) $ABCDEFGH$;(ii) $CDBAFEHG$;(iii) $DCBFHGEA$. 也见图 10-50(b)和图 10-51(b),而 END=14.

	1	2	3	4	5	6	7	8	9	10
INFO	A	C	E	G			B	D	F	H
LEFT	7	0	4	0			8	0	0	0
RIGHT	2	9	10	0			3	0	0	0

(a)

	1	2	3	4	5	6	7	8	9	10
INFO	A	C	E	G			B	D	F	H
LEFT	7	0	9	10			2	0	0	0
RIGHT	3	8	4	0			0	0	0	0

(b)

图 10-50

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
(a) TREE	A	B	C	D	E		F			G	H					
(b) TREE	A	B	E	C		F	G		D					H		

图 10-51

10.23 (a) 见图 10-52.

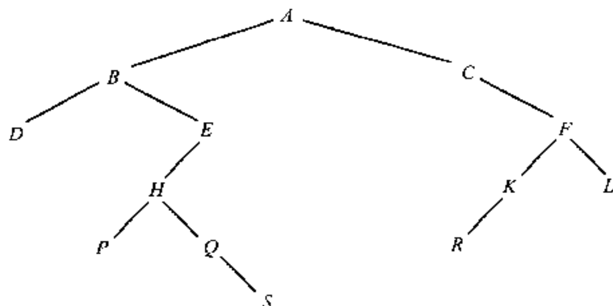


图 10-52

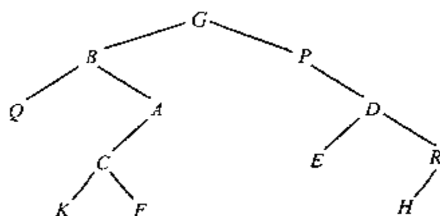


图 10-53

(b) (i) $ABDEHPQSCFKRL$;(ii) $DBPHQSEACRKFL$;(iii) $DPSQHEBRKLFCA$.

(c) $d=6$;因此 $32 \leq \text{END} < 64$. 特别地,END=43.

10.24 (a) 见图 10-53.

(b) (i) $d=5$;(ii) Q,A,C,K,F.

(c) Q,K,F,E,H.

10.25 见图 10-54,前序: $* \uparrow + x * 3 y 4 - a 2 * b$.

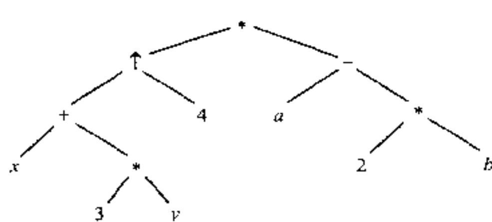


图 10-54

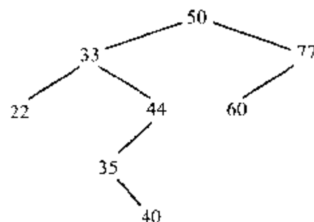


图 10-55

10.26　见图 10-55.

10.27　见图 10-56.

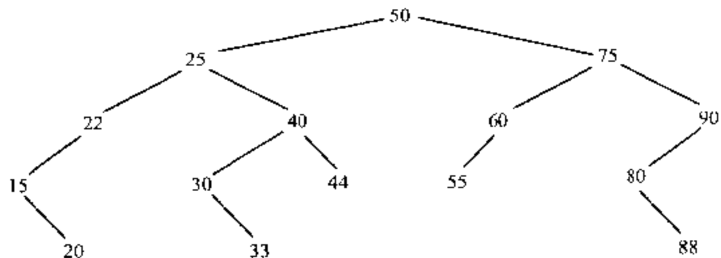


图 10-56

10.28　见图 10-57.

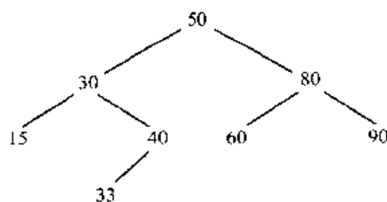
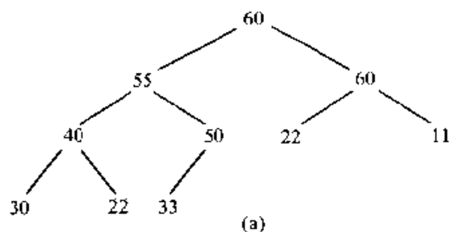


图 10-57

10.29　(a) TREE:30,50,22,33,40,60,11,60,22,55.

(b) 见图 10-58(a).

(c) 见图 10-58(b).



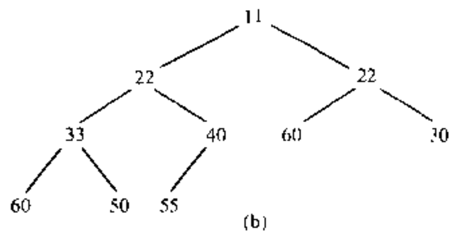


图 10-58

10.30　A:00;B:0100;C:10;D:011;E:01010;F:01011;G:11.

10.31　$P=329$.

10.32　A:000;B:00101;C:10;D:11;E:01;F:00100;G:0011;$P=252$.

10.33　见图 10-59.

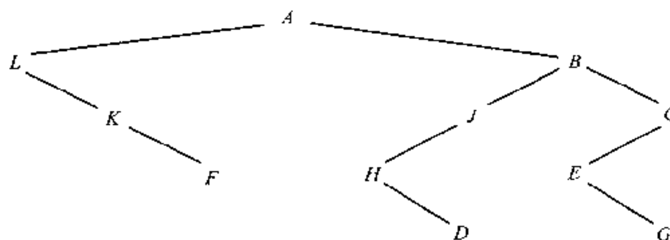


图 10-59

第十一章　整数的性质

11.1　引　言

本章主要研究自然数(或正整数)和整数的一些基本性质.

自然数集 $N=\{1,2,3,\cdots\}$.

整数集 $Z=\{\cdots,-2,-1,0,1,2,\cdots\}$.

假定这些数集关于加法和乘法有下列简单规律:

(a) 结合律:

$$(a+b)+c=a+(b+c),\quad (ab)c=a(bc).$$

(b) 交换律:

$$a+b=b+a,\quad ab=ba.$$

(c) 分配律:

$$a(b+c)=ab+ac.$$

(d) 加法单位元和乘法单位元:

$$a+0=0+a=a,\quad a\cdot 1=1\cdot a=a.$$

(e) 对于任何元素 a 都有其加法逆元 $-a$,即

$$a+(-a)=(-a)+a=0.$$

下一章将证明其他的一些数学结构也具有以上性质。这里将再次讨论数学归纳法(1.10节),因为它是区分整数和其他数学结构的一个最基本的性质。另外我们将在问题 11.34 中证明下面的定理.

算术基本定理　每一个正整数 $n(n>1)$ 都可以惟一地写成素数的积.

这个定理早在欧几里得的《原本》中出现过,我们先引入证明这个重要定理所需的一些概念和方法.

11.2　序、不等式与绝对值

本节讨论序和绝对值的基本性质.

序

设 a、b 为整数,如果 $b-a$ 的差是正的,即 $b-a\in\mathbf{N}$,我们就说 a 小于 b,记为 $a<b$.

注意这里是用正整数 $\mathbf{N}$ 来定义整数集 $\mathbf{Z}$ 中的序,所有的顺序关系的常用性质都可用下列两则 $\mathbf{Z}$ 整数 $\mathbf{N}$ 的性质派生出来.

[P₁]　如果 a、$b\in\mathbf{N}$,那么 $a+b\in\mathbf{N}$,$ab\in\mathbf{N}$.

[P₂]　对于任意整数 a,或者 $a\in\mathbf{N}$,或者 $a=0$,或者 $-a\in\mathbf{N}$.

下面的记号也经常用到:

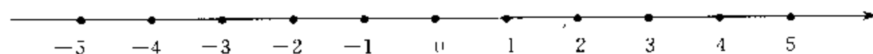
$a>b$,即 $b<a$,读作 a 大于 b.

$a\leqslant b$,即 $a<b$ 或 $a=b$,读作 a 小于等于 b.

$a\geqslant b$,即 $b\leqslant a$,读作 a 大于等于 b.

为了和等于关系"="区别这里把 $<$,$>$,$\leqslant$ 和 $\geqslant$ 叫做不等关系。

读者一定很熟悉数轴 R,即用一直线上的点代表数:



当且仅当在数轴上 a 位于 b 的左边时,记 $a<b$. 例如:

$$2<5;\quad -6<-3;\quad 4\leqslant 4;\quad 5>-8;\quad 6\geqslant 0;\quad -7\leqslant 0.$$

当且仅当 $a>0$ 时，说 a 是正的，当且仅当 $a<0$ 时，说 a 是负的.

下面是不等式的基本性质.

命题 11.1　关系 $\leqslant$ 在整数集 $\mathbf{Z}$ 中有下列性质：

(i) $a\leqslant a$，对任意的整数 a.

(ii) 如果 $a\leqslant b$ 且 $b\leqslant a$ 则 $a=b$.

(iii) 如果 $a\leqslant b$ 且 $b\leqslant c$ 则 $a\leqslant c$.

命题 11.2(三分律)　对于任何整数 a 和 b，恰有下列关系之一被满足：

$$a<b,\quad a=b,\quad \text{或 } a>b.$$

命题 11.3　假定 $a\leqslant b$，c 为任意整数. 则

(i) $a+c\leqslant b+c$.

(ii) $ac\leqslant bc(c>0)$；$ac\geqslant bc(c<0)$.

(命题 11.3 在问题 11.6 中证明)

绝对值

整数 a 的绝对值记为 $|a|$，通常定义为：

$$|a|=\begin{cases}a, & \text{若 } a\geqslant 0,\\ -a, & \text{若 } a<0.\end{cases}$$

因此除了 $a=0$ 之外，$|a|>0$. $|a|$ 的几何意义为点 a 到原点的距离，并且将 $|a-b|=|b-a|$ 视为两点 a,b 之间的距离. 例如：

(a) $|-3|=3$；　$|7|=7$；　$|-13|=13$.

(b) $|2-7|=|-5|=5$ 和 $|7-2|=|5|=5$.

(c) $|-3-8|=|-11|=11$.

下面是绝对值函数的一些性质.（问题 11.7 和 8 证明了(iii)和(iv)）

命题 11.4　设 a、b 为任意整数，则

(i) $|a|\geqslant 0$，当且仅当 $a=0$ 时 $|a|=0$.

(ii) $-|a|\leqslant a\leqslant |a|$.

(iii) $|ab|=|a||b|$.

(iv) $|a\pm b|\leqslant |a|+|b|$.

(v) $||a|-|b||\leqslant |a\pm b|$.

11.3　数学归纳法

以下叙述的数学归纳法原理本质上是正整数 $\mathbf{N}$ 从 1 开始，余下的是通过依次加 1 得到的，亦即从 1 开始，然后 $2=1+1$，然后 $3=2+1$，然后 $4=3+1$ 等等. 这个方法使模糊说法"等等"变得准确了。

数学归纳法原理　设 S 是一个正整数集合且有下列两个性质：

(i) $1\in S$.

(ii) 若 $k\in S$，则 $k+1\in S$.

那么 S 是所有正整数构成的集合.

这里不证明这个原理. 事实上，当自然数由公理化方法给出时，这个原理可作为一个公理。

下面是上述原理的一个等价形式，它常用于证明定理.

数学归纳法原理　设 P 是定义在整数 $n\geqslant 1$ 上的一个命题，使得

(i) $P(1)$ 成立.

(ii) 当 $P(n)$ 成立时 $P(n+1)$ 也成立.

那么命题 P 对于任意整数 $n(n\geqslant 1)$ 都成立.

例 11.1　(a) 设 P 表示命题：前 n 个奇数之和为 n^2 即

$$P(n)\ 1+3+5+\cdots+(2n-1)=n^2$$

例 11.2 (a) 设 $a=4461, b=16$. 通过长除法得 $q=278$ 和 $r=13$,如图 11-2(a)所示.

$$4461 = 16(278) + 13$$

即 $a=bq+r$.

(b) 设 $a=-262, b=3$,首先用 3 除 262,如图 11-2(b)所示. 这样得到了一个商 87 和余数 1;由此

$$262 = 3(87) + 1.$$

我们要求的是 $a=-262$ 所以在等式两边同乘 -1 得

$$-262 = 3(-87) - 1.$$

但是 -1 是负的所以不能作为 r;我们可以通过加负 b 调整如下:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2.$$

因此,$q=-88$, $r=2$.

(c) 设 $b=2$,则任一整数 a 都可写成如下形式

$$a = 2q + r, \quad 0 \leqslant r < 2.$$

于是 r 只能为 0 或 1,因此每一个整数都可写成 $2k$ 或 $2k+1$. 形如 $2k$ 的整数称为偶数,形如 $2k+1$ 的整数称为奇数(通常,偶数是用能被 2 整除定义的,其他的数被称为奇数.)从而带余除法证明了每一个奇数有形式 $2k+1$.

```
     278              87
16)4461           3)262
   32               24
   126               22
   112               21
    141               1
    128
     13
   (a)              (b)
```

图 11-2

11.5 整除,素数

设 a、b 为整数且 $a \neq 0$,假设存在整数 C 使得 $ac=b$,我们就称 a 整除 b 或者说 b 被 a 整除,记作

$$a \mid b$$

我们也说 b 是 a 的倍数或者 a 是 b 的因子. 如果 a 不能整除 b 我们记作 $a \nmid b$.

例 11.3 (a) $3 \mid 6$,因为 $3 \cdot 2=6$,$-4 \mid 28$,因为 $(-4)(-7)=28$.

(b) 因子:

(i) 1 的因子有 ± 1;

(ii) 2 的因子是 $\pm 1, \pm 2$;

(iii) 4 的因子是 $\pm 1, \pm 2, \pm 4$;

(iv) 5 的因子是 $\pm 1, \pm 5$;

(v) 7 的因子是 $\pm 1, \pm 7$;

(vi) 9 的因子是 ± 1、± 3、± 9.

(c) 如果 $a \neq 0$,则 $a \mid 0$,因为 $a \cdot 0=0$

(d) 任一整数 a 都能被 ± 1 和 $\pm a$ 整除,它们有时被称之为 a 的平凡因子.

下面的定理给出整除的基本性质(问题 11.28 给出证明).

定理 11.8 设 a, b, c 为整数.

(i) 如果 $a \mid b$ 且 $b \mid c$,则 $a \mid c$.

(ii) 如果 $a \mid b$,那么对于任一整数 x,$a \mid bx$.

(iii) 如果 $a \mid b$ 且 $a \mid c$,则 $a \mid (b+c)$ 且 $a \mid (b-c)$.

(iv) 如果 $a \mid b$ 且 $b \neq 0$,则 $a = \pm b$ 或 $|a| < |b|$.

(v) 如果 $a \mid b$ 且 $b \mid a$,则 $|a| = |b|$ 即 $a = \pm b$.

(vi) 如果 $a|1$ 则 $a=\pm 1$.

由(ii)和(iii),我们有下面一个重要结论.

推论 11.9　设 $a|b$ 且 $a|c$,则对于任意的整数 x 和 y 有 $a|(bx+cy)$.

我们称表达式 $bx+cy$ 为 b,c 的线性组合.

素数

如果一个正整数 $p(>1)$ 只有因子 ± 1 和 $\pm p$,即 p 有平凡因子,我们称其为素数.如果正整数 $n(>1)$ 不是素数,则称其为合数.注意到,如果 $n(>1)$ 是合数,那么 $n=ab$,其中 $1<a,b<n$.

例 11.4　(a) 整数 2 和 7 是素数,而 $6=2\cdot 3$ 和 $15=3\cdot 5$ 是合数.

(b) 下面是 50 以内的素数.

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47.$$

(c) 尽管 21,24 和 1729 不是素数,但它们都可写成素数的积.

$$21=3\cdot 7,\quad 24=2\cdot 2\cdot 2\cdot 3=2^3\cdot 3,\quad 1729=7\cdot 13\cdot 19$$

算术基本定理指出任意大于 1 的整数都可以写成素数的积,并且从本质上讲写法是惟一的.算术基本定理是一个深刻的证明有些难度的定理,但是在证明这种积存在这一点上,利用归纳法很容易.

定理 11.10　任意大于 1 的整数都可写成素数的积.

注意,一个积可能只有一个因子组成,所以素数 p 本身是素数的积.由于定理 11.10 相对比较简单,我们在这里给出证明.

证明　用数学归纳法.当 $n=2$ 时,因为 2 是素数,所以 n 就是一个素数积.假设$n>2$时,定理对于小于 n 的正整数成立,如果 n 是素数,则 n 是一个素数积.如果 n 是合数,则 $n=ab$,其中 $a,b<n$,由数学归纳法得 a 和 b 是素数积,因此 $n=ab$ 也是素数积.

欧几里得证明了算术基本定理,也被问及是否存在一个最大的素数.他这样回答了这个问题:

定理 11.11　没有最大的素数,也就是说存在无限多个素数.

证明　假设只有有限个素数,设它们为 $p_1,p_2,\cdots,p_m$,考虑整数

$$n=p_1p_2\cdots p_m+1.$$

由于 n 是素数积(定理 11.10),所以 n 一定被素数整除,不妨设其为 p_k,注意到 p_k 也整除 $p_1p_2\cdots p_m$,因此 p_k 整除

$$n-p_1p_2\cdots p_m=1.$$

这是不可能的,所以 n 被其他的某个素数整除.这与假设只有 $p_1,p_2,\cdots,p_m$ 是素数矛盾.因此素数的个数是无限的,定理得证.

11.6　最大公因数、带余除法

设 a,b 是整数且不全为 0,整数 d 称为 a,b 的公因子,如果 $d|a$ 且 $d|b$.注意 1 是 a 和 b 的正的公因子,a 和 b 的任何公因子都不能大于 $|a|$ 和 $|b|$,这样就存在 a 和 b 的一个最大的公因子,记为

$$\gcd(a,b)$$

称之为 a,b 的最大公因数.

例 11.5　(a) 12 和 18 的公因子有 $\pm 1,\pm 2,\pm 3,\pm 6$,因此

$$\gcd(12,18)=6.$$

类似地,

$$\gcd(12,-18)=6,\gcd(12,-16)=4,\gcd(29,15)=1,\gcd(14,49)=7.$$

(b) 对于任意整数 a,有 $\gcd(1,a)=1$.

(c) 对于任意素数 p,有

$$\gcd(p,a)=p\quad 或\quad \gcd(p,a)=1.$$

结果取决于 $p|a$ 或 $p\nmid a$.

(d) 设 a 是正数,那么 $a|b$ 当且仅当 $\gcd(a,b)=a$.

下面的定理(证明在问题 11.30 中)给出了最大公因数的另一个特征.

定理 11.12 设 d 是形如 $ax+by$ 的最小的正整数,则 $d=\gcd(a,b)$.

推论 11.13 设 $d=\gcd(a,b)$,则一定存在整数 x 和 y 使得 $d=ax+by$.

下面是刻画最大公因数的另一种方法,这种方法不使用不等关系.

定理 11.14 一个正整数 $d=\gcd(a,b)$ 当且仅当 d 有下列两个性质:

(1) d 既整除 a,又整除 b.

(2) 如果 c 既整除 a 又整除 b,那么 $c|d$.

下面是最大公因数的简单性质:

(a) $\gcd(a,b)=\gcd(b,a)$.

(b) 如果 $x>0$,那么 $\gcd(ax,bx)=x\cdot\gcd(a,b)$.

(c) 如果 $d=\gcd(a,b)$,那么 $\gcd(a|d,b|d)=1$.

(d) 对于任意整数 x,$\gcd(a,b)=\gcd(a,b+ax)$.

带余除法

设 a,b 为整数且 $d=\gcd(a,b)$. 人们总可以通过列出 a 和 b 的所有因子,然后选择最大公因子来发现 d. 设 $n=a+b$,计算因子的个数,这种代数方法的复杂性为 $f(n)=O(\sqrt{n})$. 同样我们也没有给出任何方法来求 x,y,使得

$$d=ax+by$$

下面我们介绍一种非常有效但性质复杂的代数方法 $f(n)=O(\log n)$,求最大公因数 $d=\gcd(a,b)$ 和 x,y.

这种代数方法我们称之为带余除法,它是由反复运用长除法构成的. 我们用一个例子来说明这种方法.

例 11.6 设 $a=540,b=168$. 我们通过用 a 除以 b,然后重复地用余数除以除数直到余数为零的方法来求 $d=\gcd(a,b)$. 具体步骤如图 11-3 所示. 最后一个非零余数是 12,于是

$$12=\gcd(540,168).$$

这根据以下事实.

$$\gcd(540,168)=\gcd(168,36)=\gcd(36,24)=\gcd(24,12)=12.$$

```
      3            4           1          2
168)540        36)168      24)36      12)24
    504            144         24         24
     36             24         12          0
```

图 11-3

下一步我们来求 x,y 使得

$$12=540x+168y.$$

图 11-3 中的前三个商满足下列等式:

(1) $540=3(168)+36$ 或 $36=540-3(168)$.

(2) $168=4(36)+24$ 或 $24=168-4(36)$.

(3) $36=1(24)+12$ 或 $12=36-1(24)$.

由等式(3)得 12 是 36 和 24 的线性组合. 我们用(2)式来代替(3)式中的 24,可以把 12 写成 168 和 36 的线性组合如下:

(4) $12=36-1[168-4(36)]=36-1(168)+4(36)$

$=5(36)-1(168)$.

将(1)代入(4),可以将 12 写成 168 和 540 的线性组合如下:

$$\begin{aligned}12 &= 5[540 - 3(168)] - 1(168)\\ &= 5(540) - 15(168) - 1(168)\\ &= 5(540) - 16(168).\end{aligned}$$

这就是我们所要求的线性组合,因此 $x=5$　$y=16$.

最小公倍数

设 a 和 b 是非零整数,$|ab|$ 就是 a 和 b 的一个正的公倍数.因此存在 a,b 的一个最小的公倍数,记为

$$\operatorname{lcm}(a,b).$$

我们称之为 a 和 b 的最小公倍数.

例 11.7　(a) $\operatorname{lcm}(2,3)=6$;　$\operatorname{lcm}(4,6)=12$;　$\operatorname{lcm}(9,10)=90$.

(b) 对于任意正整数 a 有 $\operatorname{lcm}(1,a)=a$.

(c) 对于任意的素数 p 和正整数 a 有

$$\operatorname{lcm}(p,a) = a \quad 或 \quad \operatorname{lcm}(p,a) = ap.$$

结果取决于 $p|a$ 或 $p|a$.

(d) 设 a 和 b 是正整数,那么 $a|b$ 当且仅当 $\operatorname{lcm}(a,b)=b$.

下面的定理给出了最大公因数与最小公倍数之间的一个重要关系.

定理 11.15　设 a 和 b 是非零整数,则

$$\operatorname{lcm}(a,b) = \frac{|ab|}{\gcd(a,b)}.$$

11.7　算术基本定理

下面讨论算术基本定理,首先我们需要介绍互素的概念.

互素

两个整数 a 和 b 称之为互素,如果

$$\gcd(a,b) = 1.$$

因此如果 a 和 b 互素,那么存在 x 和 y 使得

$$ax + by = 1.$$

反之,如果 $ax+by=1$,则 a,b 互素.

例 11.8　(a) 观察得

$$\gcd(12,35) = 1,\quad \gcd(49,18) = 1,\quad \gcd(21,64) = 1,\quad \gcd(-28,45) = 1.$$

(b) 如果 p 和 q 是两相异的素数,则 $\gcd(p,q)=1$.

(c) 对于任意整数 a,我们有

$$\gcd(a,a+1) = 1.$$

此据 a 和 $a+1$ 的任何公因子必整除它们的差 $(a+1)-a=1$ 而得.

由于下面的结果互素关系尤为重要,我们将给出第二个定理的证明.

定理 11.16　设 $\gcd(a,b)=1$,a 和 b 都整除 c,则 ab 整除 c.

定理 11.17　设 $a|bc$ 且 $\gcd(a,b)=1$,则 $a|c$.

证明　因为 $\gcd(a,b)=1$,所以存在 x 和 y 使得 $ax+by=1$,等式乘以 c 得

$$acx + bcy = c.$$

我们有 $a|acx$ 且 $a|bcy$,根据假设 $a|bc$.因此 a 整除和 $acx+bcy=c$.

推论 11.18　设一素数 p 整除积 ab,则 $p|a$ 或 $p|b$.

这个推论来源于欧几里得,实际上它是欧几里得证明算术基本定理的基础.

算术基本定理

定理 11.10 指出每一个整数是素数的积.但是不同素数的积能否得到同样的数呢?显然我们可以重新安排素数因子的顺序,例如

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5.$$

算术基本定理(在问题 11.35 中证明)指出如果两个“不同的”积得到同样的数,仅仅是乘积因式重新排序而已.

定理 11.19(算术基本定理)　每个整数 $n(>1)$都能被惟一的(不计顺序)表示成素数的积.

n 的分解式中的素数不一定要不同.因此把所有相等的素数结合起来很有用,n 可表示为以下形式

$$n = p_1^{m_1} p_2^{m_2} p_r^{m_r}.$$

式中 m_i 是正的,且 $p_1 < p_2 < \cdots < p_r$.上式称为 n 的标准分解式.

例 11.9　设 $a = 2^4 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13$,$b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$.求 $d = \gcd(a,b)$,$m = \mathrm{lcm}(a,b)$.

(a) 先求 $d = \gcd(a,b)$.那些在 a 和 b 中都出现的素数 p_i,如 2,3 和 11 将在 d 中出现,p_i 在 d 中的指数取 a 和 b 中较小的一个,因此

$$d = \gcd(a,b) = 2^3 \cdot 3^2 \cdot 11 = 792.$$

(b) 下一步求 $m = \mathrm{lcm}(a,b)$.那些在 a 或者 b 中出现的素数 p_i,如 2,3,5,7,11,13 和 17 将在 m 中也出现,P_i 在 m 中的指数取 a 和 b 中较大的一个,因此

$$m = \mathrm{lcm}(a,b)$$
$$= 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17.$$

我们都习惯于用算术基本定理,以致于认为它无需证明,而欧几里得发现它需要证明,并且第一个证明了这个定理.我们通过举一个不满足这个定理的数组来强调这个定理的重要性.

例 11.10　设 F 是形如 $3x+1$ 的正整数集,F 由下列数字构成

$$1,4,7,10,13,16,19,22,\cdots.$$

注意到 F 中两数字的积仍在 F 中,因为

$$(3x+1)(3y+1) = 9xy + 3x + 3y + 1 = 3(3xy + x - y) + 1.$$

关于素数的定义在 F 中同样有意义,F 中开始的几个素数为

$$4,7,10,13,19,22,25,\cdots.$$

尽管 $4 = 2 \cdot 2$,但数字 2 不在 F 中,4 在 F 中是素数,因为 4 除了 1 和 4 外无其他因子.类似地,10,22,25,…在 F 中也为素数,注意 $100 = 3(33)+1$ 属于 F,但是 100 在 F 中有两个在本质上不同的 F 中素数的分解式:

$$100 = 4 \cdot 25,\quad 100 = 10 \cdot 10.$$

因此 F 中数的未必只有惟一的 F 中素数的分解式.

11.8　同余关系

设 m 是一正整数,我们说 a,b 模 m 同余,记为

$$a \equiv b(\text{modulo } m) \text{ 或简写为 } a \equiv b(\text{mod } m)$$

如果 m 能整除 $a-b$,整数 m 称为模.不能整除时记为 $a \not\equiv b(\text{mod } m)$.例如:

(i) $87 \equiv 23(\text{mod } 4)$,因为 4 整除 $87-23=64$.

(ii) $67 \equiv 1(\text{mod } 6)$,因为 6 整除 $67-1=66$.

(iii) $72 \equiv -5(\text{mod } 7)$,因为 7 整除 $72-(-5)=77$.

(iv) $27 \not\equiv 8(\text{mod } 9)$,因为 9 不整除 $27-8=19$.

下面的定理(在问题 11.40 中证明)指出模 m 同余是一个等价关系.

定理 11.20　设 m 是一正整数,那么

(i) 对于任意整数 a,有 $a \equiv a(\text{mod } m)$.

(ii) 如果 $a \equiv b(\text{mod } m)$,那么 $b \equiv a(\text{mod } m)$.

(iii) 如果 $a \equiv b(\text{mod } m)$,$b \equiv c(\text{mod } m)$,那么 $a \equiv c(\text{mod } m)$.

注　设 m 是正数，a 是任意整数. 由带余除法，存在整数 q 和 $r(0\leqslant r<m)$ 使得 $a=mq+r$. 因此

$$mq=a-r \text{ 或 } m\mid(a-r) \text{ 或 } a\equiv r(\bmod m).$$

于是

(1) 任意整数 a 模 m 都与下列集合中惟一的一个整数同余.

$$\{0,1,2,\cdots,m-1\}.$$

惟一性可由 m 不能整除集合中两个整数的差推得.

(2) 任意两个整数 a 和 b 模 m 同余，当且仅当它们除以 m 所得余数相同.

剩余类

既然模 m 同余是一等价关系，那么它就把整数集 $\mathbf{Z}$ 分成了互不相交的等价类，我们称之为模 m 剩余类. 由以上表述，一个剩余类由所有的被 m 除余数相同的数组成，因此有 m 个这样的剩余类并且每一个剩余类都恰恰含有余数集中的一个整数，

$$\{0,1,\cdots,m-1\}.$$

一般地，一个由 m 个整数组成的集合 $\{a_1,a_2,a_3\cdots a_m\}$ 称为模 m 的完全剩余系，如果每一个 a_i 取自一个不同的剩余类. 因此从 0 到 $m-1$ 的整数构成了一个完全剩余系. 事实上，任何 m 个连续的整数都构成一个模 m 的完全剩余系.

记号 $[x]_m$ 或 $[x]$ 表示包含 x 的模 m 的剩余类，也就是那些和 x 同余的整数，换句话说

$$[x]=\{a\in\mathbf{Z}:a\equiv x(\bmod m)\}$$

因此，剩余类可以记为

$$[0],[1],[2],\cdots,[m-1].$$

或者选择完全剩余系中的其他整数.

例 11.11　模 $m=6$ 的剩余类如下：

$$[0]=\{\cdots,-18,-12,-6,0,6,12,18\cdots\},$$
$$[3]=\{\cdots,-15,-9,-3,3,9,15,21\cdots\},$$
$$[1]=\{\cdots,-17,-11,-5,1,7,13,19\cdots\},$$
$$[4]=\{\cdots,-14,-8,-2,4,10,16,22\cdots\},$$
$$[2]=\{\cdots,-16,-10,-4,2,8,14,20,\cdots\},$$
$$[5]=\{\cdots,-13,-7,-1,5,11,17,23\cdots\}.$$

注意到 $\{-2,-1,0,1,2,3\}$ 也是模 6 的完全剩余系.

同余的计算

下面的定理（在问题 11.41 中证明）指出在加法和乘法下，同余关系很像等于关系.

定理 11.21　设 $a\equiv c(\bmod m)$，$b\equiv d(\bmod m)$. 那么

(i) $a+b\equiv c+d(\bmod m)$.

(ii) $a\cdot b\equiv c\cdot d(\bmod m)$.

注　设 $p(x)$ 是一整系数多项式，如果 $S\equiv t(\bmod m)$，则反复运用上述定理可以证明 $p(s)\equiv p(t)(\bmod m)$.

例 11.12　观察 $2\equiv 8(\bmod 6)$ 和 $5\equiv 41(\bmod 6)$，那么

(i) $2+5\equiv 8+41(\bmod 6)$ 或 $7\equiv 49(\bmod 6)$.

(ii) $2\cdot 5\equiv 8\cdot 41(\bmod 6)$ 或 $10\equiv 328(\bmod 6)$.

设 $P(x)=3x^2-7x+5$. 那么

$$p(2)=12-14+5=3,p(8)=192-56+5=141$$

因此 $3\equiv 141(\bmod 6)$.

剩余类的运算

模 m 剩余类的加法和乘法定义如下：

$$[a]+[b]=[a+b],[a]\cdot[b]=[ab].$$

考虑模 $m=6$ 的剩余类，

$$[0],\quad [1],\quad [2],\quad [3],\quad [4],\quad [5].$$

则

$$[2]+[3]=[5],[4]+[5]=[9]=[3],[2]\cdot[2]=[4],[2][5]=[10]=[4].$$

定理 11.21 的指出上述定义是有意义的，即剩余类的和与积与代表元的选取无关.

模 m 剩余类只有 m 个，因此当 m 较小时容易写出它们的加法表和乘法表. 图 11－4 指出了模 $m=6$ 的剩余类的加法表和乘法表. 为方便计省去了方括号，而直接用数字 0,1,2,3,4,5 表示剩余类.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

图 11－4

模 m 的整数 $\mathbf{Z}_m$

模 m 的整数记为 $\mathbf{Z}_m$，指的是集合

$$\mathbf{Z}_m=\{0,1,2,3,\cdots,m-1\}.$$

其上加法和乘法是通过模 m 的运算定义的，换句话说是剩余类上的相应运算. 例如，图 11－4 也可以看做是 $\mathbf{Z}_6$ 的乘法表和加法表. 这意味着

> $\mathbf{Z}_m$ 与模 m 剩余类的运算没有本质的区别，因此可以通用.

同余的消去律

回忆整数满足：

> 消去律：如果 $ab=ac$ 且 $a\neq0$，则 $b=c$.

一般的运算和模 m 运算之间最大的不同是上面的消去律对于同余关系不满足. 比如

$$3\cdot1\equiv3\cdot5(\bmod 6)\quad 但\quad 1\not\equiv5(\bmod 6).$$

也就是说，即使 $3\not\equiv0(\bmod 6)$ 我们也不能消去 3，但是对于同余关系我们有修正的消去律.

定理 11.22（修正消去律）　设 $ab\equiv ac(\bmod m)$　$\gcd(a,m)=1$，那么 $b\equiv c(\bmod m)$.

上面的定理是下述更一般结论的推论（在问题 11.44 中证明）.

定理 11.23　设 $a,b\equiv ac(\bmod m)$，$d=\gcd(a,m)$，则 $b\equiv c(\bmod m/d)$

例 11.13　考虑下面的同余式

$$6\equiv36(\bmod 10).\tag{1}$$

因为 3 和模 10 互素，我们可以在(1)式的两端同除以 3，得

$$2\equiv12(\bmod 10).$$

注意到我们不能在(1)式两边同除以 6，因为

$$1\not\equiv6(\bmod 10).$$

但由定理 11.23，我们可以在(1)式两端同除以 6 同时将模除以 $2=\gcd(6,10)$，即

$$1\equiv 6 \pmod 5.$$

注 设 p 为素数，则整数 1 到 $p-1$ 都与 p 互素，这样通常的消去律当模为素数 p 时满足，也就是说

如果 $ab\equiv ac \pmod p$ 且 $a\not\equiv 0 \pmod p$，那么 $b\equiv c \pmod p$.

这样 $\mathbf{Z}p$，模素数 p 的整数在数论上起到了特殊的作用.

简化剩余系和欧拉函数

修正消去律定理 11.22 表明那些与模 m 互素的整数起着特殊的作用. 注意到 a 与 m 互素当且仅当剩余类$[a]$中的每一个元素都与 m 互素，于是我们可以讨论与 m 互素的剩余类.

与 m 互素的剩余类的个数即从 1 到 m(不包括 m)中与 m 互素的数的个数记为

$$\varnothing(m).$$

函数$\varnothing(m)$称为*欧拉函数*，1 到 m 中与 m 互素的整数，或更一般地，任何$\varnothing(m)$个与 m 互素的不同余的整数列称为*模 m 的简化剩余系*.

例 11.14 (a) 考虑模 $m=15$，在 1 与 15 之间有 8 个与 15 互素的整数

$$1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14.$$

这样$\varnothing(15)=8$，并且上面的 8 个整数组成了一个模 15 的简化剩余系.

(b)考虑任意素数 p，所有的数 $1,2\cdots p-1$ 与 p 互素，即$\varnothing(p)=p-1$.

一个定义域为正整数 $\mathbf{N}$ 的函数 f 称为*可乘的*，如果当 a 和 b 互素时，有

$$f(ab)=f(a)f(b).$$

下面的定理(在问题 11.51 中证明)是有用的.

定理 11.24 欧拉函数是可乘的，即若 a,b 互素，那么

$$\varnothing(ab)=\varnothing(a)\varnothing(b).$$

11.9 同余式

一个*同余多项式方程*或称一个*同余方程*(关于未知数 x)是如下形式的方程

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1+a_0\equiv 0 \pmod m \qquad (*)$$

这样的一个方程称为 n 次的，如果 $a_n\not\equiv 0 \pmod m$.

设 $s\equiv t \pmod m$，那么 s 是方程(*)的解当且仅当 t 是(*)的解. 这样(*)解的个数即为不同余的解的个数，即在下面集合中解的个数

$$\{0,1,2,\cdots,m-1\}.$$

当然，这些解总可以通过一个一个地试得到，也就是说，把这 m 个数当中的每一个数代入方程(*)中看看它是否确实满足方程.

方程(*)的*完全解*是不同余的解的最大集合，而方程(*)的*一般解*则是所有满足(*)的解，一般解可以通过把所有 m 的倍数加到完全解上得到.

例 11.15 考虑下列方程

(a) $x^2+x+1\equiv 0 \pmod 4$.

(b) $x^2+3\equiv 0 \pmod 6$.

(c) $x^2-1\equiv 0 \pmod 8$.

我们通过试的方法来求解.

(a) 由于 0,1,2,3 都不满足方程，所以无解.

(b) 在 $0,1,\cdots,5$ 中只有 3 是解，这样一般解由形如 $3+6k(k\in\mathbf{Z})$ 的整数组成.

(c) 有四个解，1,3,5 和 7，这说明一个 n 次同余方程可以有多于 n 个的解.

我们强调研究同余方程不仅仅是为了求解，它总可以通过试的方法来求. 我们的主

要兴趣是，不断探索技术帮助我们求解这种方程的技术，并探讨在何种条件下解存在且有多少个解. 这一点对于下面要研究的线性同余方程成立. 我们还将讨论中国剩余定理，从本质上说它是一个线性同余方程组.

注 1 同余方程的系数总可以在模 m 下化简，因为将会得到一个等价方程，即同解方程. 例如，

$15x^2+28x+14\equiv 0(\bmod 6)$，$3x^2+4x+2\equiv 0(\bmod 6)$，$3x^2-2x+2\equiv 0(\bmod 6)$，

是等价方程，因为系数模 $m=6$ 同余. 通常我们在 0 到 $m-1$ 或 $-m/2$ 到 $m/2$ 之间选择系数.

注 2 因为我们是在模 m 剩余类中寻找方程(*)的解，而不是在所有的整数中，所以可把方程(*)看做是 $\mathbf{Z}m$ 上的方程而不是 $\mathbf{Z}$ 上的方程. 在此意义下方程(*)解的个数是指 $\mathbf{Z}m$ 中解的个数.

线性同余方程：$ax\equiv 1(\bmod m)$

首先，我们考虑特殊的线性同余方程

$$ax\equiv 1(\bmod m). \qquad (**)$$

这里 $a\not\equiv 0(\bmod m)$. 有下面的定理(在问题 11.65 中证明).

定理 11.25 如果 a 和 m 互素，那么 $ax\equiv 1(\bmod m)$ 有惟一解，否则无解.

例 11.16 (a) 考虑同余方程

$$6x\equiv 1(\bmod 33).$$

注意到 $\gcd(6,33)=3$，所以该方程无解.

(b) 考虑同余方程

$$7x\equiv 1(\bmod 9).$$

这里 $\gcd(7,9)=1$；因此该方程有惟一解，尝试 0，1，…8，我们发现

$$7(4)=28\equiv 1(\bmod 9).$$

因此 $x=4$ 是惟一解.（一般解是 $4+9k$，$k\in\mathbf{Z}$.）

假设方程(**)有解，也就是说 $\gcd(a,m)=1$，并且模 m 很大，那么欧几里得带余除法可以用来求解. 特别地，我们用带余除法求 x_0，y_0 使得

$$ax_0+my_0=1.$$

由此得出 $ax_0\equiv 1(\bmod m)$，也就是说 x_0 是方程(**)的一个解.

例 11.17 考虑下面的同余方程：

$$81x\equiv 1(\bmod 256).$$

利用带余除法，可得 $\gcd(81,256)=1$，因此方程有惟一解. 由于模 $m=256$ 相对较大，试或许不是一个求解的好方法，因此对于 $a=81$ 和 $m=256$ 运用带余除法. 如例 11.6，求得 $x_0=-25$ $y_0=7$ 使得

$$81x_0+256y_0=1.$$

这就意味着 $x_0=-25$ 是方程的解，再加上 256 得到处于 0 和 256 之间的惟一解

$$x=231$$

线性同余方程：$ax\equiv b(\bmod m)$

现在考虑更一般的同余方程

$$ax\equiv b(\bmod m). \qquad (***)$$

$a\not\equiv 0(\bmod m)$. 首先考虑 a 和 m 互素的情况(在问题 11.66 中证明).

定理 11.26 设 a 和 m 互素，那么 $ax\equiv b(\bmod m)$ 有惟一解. 另外，如果 s 是 $ax\equiv 1(\bmod m)$ 的惟一解，那么

$$x=bs$$

是 $ax\equiv b(\bmod m)$ 的惟一解.

例 11.18 (a) 考虑同余方程

$$3x \equiv 5(\text{mod } 8).$$

因 3 和 8 互素，方程有惟一解. 试一试 0，1，…，7，得

$$3(7) = 21 = 5(\text{mod } 8).$$

于是 $x=7$ 是方程的惟一解.

(b) 考虑同余方程

$$33x \equiv 38(\text{mod } 280). \quad (1)$$

因 gcd(33，280)=1，方程有惟一解，尝试或许不太有效，因为 $m=280$ 较大. 我们用带余除数求下式的解

$$33x \equiv 1(\text{mod } 280). \quad (2)$$

即像例 11.6 一样，求得 $x_0=17$　$y_0=-2$ 是下式的一组解

$$33x_0 + 280y_0 = 1.$$

这就意味着 $S=17$ 是(2)的解，那么

$$sb = 17(38) = 646$$

是(1)的解，将 646 用 $m=280$ 除，得余数

$$x = 86,$$

为(1)在 0 与 280 之间的惟一解.（一般解是 $86+280k, k\in \mathbf{Z}$.）

下面的定理(在问题 11.67 中证明)指出了方程(* * *)的一般情况下解的过程.

定理 11.27　设方程 $ax\equiv b(\text{mod } m)$，$d=\gcd(a,m)$.

(i) 若 d 不整除 b，则 $ax\equiv b(\text{mod } m)$ 无解.

(ii) 若 d 整除 b，则 $ax\equiv b(\text{mod } m)$ 有 d 个解，它们模 m 与下列方程的惟一解同余

$$Ax \equiv B(\text{mod } M)$$

其中　$A=a/d, B=b/d, M=m/d$.

注意到，因为 $\gcd(A,M)=1$ 所以可运用定理 11.26 求定理 11.27 中的方程 $Ax\equiv B(\text{mod } M)$ 的解.

例 11.19　分别解同余方程：(a) $4x\equiv 9(\text{mod } 14)$，(b) $8x\equiv 12(\text{mod } 28)$.

(a) gcd(4，14)=2，但 2 不整除 9. 因此方程无解.

(b) 因为 $d=\gcd(8,28)=4$，$d=4$ 整除 12，所以方程有 $d=4$ 个解，将方程中每一个数都除以 $d=4$ 得同余方程

$$2x \equiv 3(\text{mod } 7)$$

有惟一解，一个一个地试 0，1，…，6 发现 5 是方程(1)的惟一解，依次将 7 的倍数加到方程(1)的解 5 上得：

$$5+7 = 12, \quad 5+2(7) = 19 \quad 5+3(7) = 26.$$

于是 5，12，19，26 就是原方程(b)的 4 个解.

注　例 11.19 中方程(1)的解是通过尝试的方法获得的，但当模 m 较大时总可以用带余除法求其惟一解，如例 11.17(见问题 11.61).

中国剩余定理

有一个古老的中国谜题，如下

有一个正整数 x，当 x 除以 3 时余数为 2；当 x 除以 5 时余数为 4；当 x 除以 7 时余数为 6，问这个数是多少？

换句话说，我们要探求下列三个同余方程的公共解

$$x \equiv 2(\text{mod } 3), x \equiv 4(\text{mod } 5), x \equiv 6(\text{mod } 7).$$

观察模 3，5 和 7 是两两互素的，下面的定理告诉我们方程组有一模 $M=3\cdot 5\cdot 7=105$ 的惟一解.

定理 11.28(中国剩余定理)　设有方程组

$$x \equiv r_1 (\mathrm{mod}\ m_1), x \equiv r_2 (\mathrm{mod}\ m_2), \cdots, x \equiv r_k (\mathrm{mod}\ m_k) \qquad (*)$$

m_i 两两互素,那么方程组有一模 $M=m_1m_2\cdots m_k$ 的惟一解.

实际上对于方程组(*)的解可以给出一个明确的公式,我们称它为命题.

命题 11.29 考虑同余方程组(*).设 $M=m_1m_2\cdots m_k$,且

$$M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \cdots, M_k = \frac{M}{m_k}$$

(那么每一对 m_i 和 m_j 互素).设 $s_1, s_2, \cdots, s_k$ 分别是下列同余方程的解

$$M_1 x \equiv 1 (\mathrm{mod} m_1), M_2 x \equiv 1 (\mathrm{mod} m_2), \cdots, M_k x \equiv 1 (\mathrm{mod} m_k).$$

那么

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \qquad (**)$$

是方程组(*)的解.

现在我们用两种方法解最初的谜题.

方法一 首先我们运用定理来解前面两个方程,

$$(a)\ x \equiv 2 (\mathrm{mod}\ 3), \quad (b) x \equiv 4 (\mathrm{mod}\ 5)$$

由定理知方程模 $M=3\cdot 5=15$ 有惟一解,在第二个方程(b)的解 $x=4$ 上,加上模 $m=5$ 的倍数,我们得到下面 3 个小于 15 方程(b)的解

$$4, \quad 9, \quad 14.$$

在方程(a)中检验每一个解,求得 14 是两方程的惟一解.

现在我们用同样的过程来解下面两个方程

$$(c)\ x \equiv 14 (\mathrm{mod}\ 15), \quad (d)\ x \equiv 6 (\mathrm{mod}\ 7).$$

由定理知方程模 $M=15\cdot 7=105$ 有惟一解,在第一个方程的解 $x=14$ 上加模 $m=15$ 的倍数,得到下面 7 个小于 105 的方程(c)的解

$$14, 29, 44, 59, 74, 89, 104.$$

在方程(d)中检验方程(c)的一些解,求得 104 是两方程的公共解,因此

$$x = 104.$$

是满足所有三个方程的最小的正整数解,这就是这个古老谜题的答案.

方法二 用上述记号,得

$$M=3\cdot 5\cdot 7=105, M_1=105/3=35, M_2=105/5=21, M_3=105/7=15.$$

我们现在来求下列方程的解

$$35x \equiv 1 (\mathrm{mod}\ 3), \quad 21x \equiv 1 (\mathrm{mod}\ 5), \quad 15x \equiv 1 (\mathrm{mod}\ 7).$$

化简 35 模 3,21 模 5 和 15 模 7,我们得到方程组

$$2x \equiv 1 (\mathrm{mod} 3), \quad x \equiv 1 (\mathrm{mod} 5), \quad x \equiv 1 (\mathrm{mod} 7).$$

这三个方程的解分别是,

$$s_1 = 2, \quad s_2 = 1, \quad s_3 = 1.$$

将它们都代入公式(**)得到原方程组的解:

$$x_0 = 35\cdot 2\cdot 2 + 21\cdot 1\cdot 4 + 15\cdot 1\cdot 6 = 314.$$

将这个解除以模 $M=105$,得到余数

$$x = 104$$

是这个谜题在 0 到 105 间的解.

注 上面的解 $s_1=2, s_2=1, s_3=1$ 是通过检验得到的,如果模很大时,可以仿照例题 11.17 用带余除法求解.

问题与解答

不等式和绝对值

11.1　在每对整数之间填入适当的符号<,>或=.

(a) 4 ____ −7,　(b) −2 ____ −9,　(c) 3^2 ____ 5,

(d) −8 ____ 3,　(e) 3^2 ____ 9,　(f) 6 ____ 8.

解　对每一对整数 a 和 b,在数轴 R 上确定它们的位置关系或计算其差 $b-a$,依据 $b-a$ 为正、负或零,分别记为

$$a<b,\quad a>b,\text{或} a=b.$$

因此

(a) $4>-7$;(b) $-2>-9$;(c) $3^2>5$;(d) $-8<3$;(e) $3^2=9$,(f) $6<8$.

11.2　计算:(a) $|-4|,|3|,|0|$;(b) $|2-5|,|-2+5|,|-2-5|$;(c) $|5-8|+|2-4|,|4-3|-|3-9|$.

解　(a) 绝对值的大小是数量但与数的符号无关. 因此

$$|-4|=4,\quad |3|=3,\quad |0|=0.$$

(b) 首先算绝对值符号内的数

$$|2-5|=|-3|=3,\quad |-2+5|=|3|=3,\quad |-2-5|=|-7|=7.$$

(c) 首先算绝对值符号内的数:

$$|5-8|+|2-4|=|-3|+|-2|=3+2=5,$$

$$|4-3|-|3-9|=|1|-|-6|=1-6=-5.$$

11.3　求每对整数之间的距离:

(a) 3 和 −7;(b) −4 和 2;(c) 1 和 9;(d) −8 和 −3;(e) 4 和 −4;(f) −5 和 −8.

解　a,b 之间的距离 d 是通过 $d=|a-b|=|b-a|$ 给出的,或者如图 11-5 所示,当 a 和 b 符号不同时 $d=|a|+|b|$;当 a 和 b 符号相同,并且 $|a|\geqslant|b|$ 时,$d=|a|-|b|$.

故(a) $d=3+7=10$;(b) $d=4+2=6$;(c) $d=9-1=8$;(d) $d=8-3=5$;(e) $d=4+4=8$;(f) $d=8-5=3$.

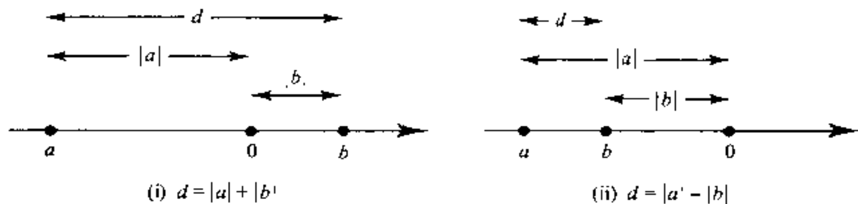


图 11-5

11.4　求分别满足:(a) $1<2n-6<14$;　(b) $2<8-3n<18$ 的所有整数 n.

解　(a) 在"三边"同加上 6 得 $7<2n<20$,然后同除以 2(或乘$\frac{1}{2}$)得 $3.5<n<10$. 因此

$$n=4,5,6,7,8,9.$$

(b) 在"三边"同加上 −8 得 $-6<-3n<10$,在三边同除以 −3(或乘$-\frac{1}{3}$),由于 −3是负的,故改变不等号的方向得.

$$2>n>-3.3\quad\text{或}\quad -3.3<n<2.$$

所以 $n=-3,-2,-1,0,1$.

11.5　证明命题 11.1(iii):如果 $a\leqslant b$ 且 $b\leqslant c$,则 $a\leqslant c$.

证　当 $a=b$ 或 $b=c$ 时,此性质显然成立,所以我们只须考虑 $a<b$ 和 $b<c$ 的情况,由 $a<b$ 和 $b<$

c，得 $b-a$ 和 $c-b$ 是正的，所以由正整数性质[P_1]，它们的和也是正的. 也就是说，

$$(b-a)+(c-b)=c-a$$

是正的，这样 $a<c$，故 $a\leqslant c$.

11.6 证明命题 11.3：设 $a\leqslant b$，c 是任意整数那么

(i) $a+c\leqslant b+c$，(ii) $ac\leqslant bc$ 当 $c>0$；但当 $c<0$ 时，$ac\geqslant bc$.

证 ☞　当 $a=b$ 时，此性质显然成立，因此我们只需考虑 $a<b$ 的情况，也就是 $b-a$ 为正时.

(i) 下面的差是正的

$$(b+c)-(a+c)=b-a,$$

因此 $a+c<b+c$.

(ii) 设 c 是正的，由正整数性质[P_1]下面的积也是正的

$$c(b-a)=bc-ac.$$

所以 $ac<bc$，现设 c 是负的，那么 $-c$ 是正的，下面的积也是正的：

$$(-c)(b-a)=ac-bc.$$

因此 $bc<ac$，即 $ac>bc$.

11.7 证明命题 11.4(iii)：$|ab|=|a||b|$.

该命题的证明分以下几种情况讨论.

证 ☞　(a) 设 $a=0$ 或 $b=0$.

那么 $|a|=0$ 或 $|b|=0$，所以 $|a||b|=0$，同样 $ab=0$. 因此　$|ab|=0=|a||b|$.

(b) 设 $a>0$ 且 $b>0$

那么 $|a|=a$，$|b|=b$. 因此 $|ab|=ab=|a||b|$.

(c) 设 $a>0$ 且 $b<0$.

那么 $|a|=a$，$|b|=-b$ 并且 $ab<0$. 因此 $|ab|=-(ab)=a(-b)=|a||b|$.

(d) 设 $a<0$ 且 $b>0$，

那么 $|a|=-a$，$|b|=b$ 并且 $ab<0$，因此 $|ab|=-(ab)=(-a)b=|a||b|$.

(e) 设 $a<0$ 且 $b<0$，

那么 $|a|=-a$，$|b|=-b$ 并且 $ab>0$，因此

$$|ab|=ab=(-a)(-b)=|a||b|.$$

11.8 证明命题 11.4(iv)：$|a\pm b|\leqslant|a|+|b|$.

证 ☞　由 $ab\leqslant|ab|=|a||b|$，得 $2ab\leqslant2|a||b|$，因此

$$(a+b)^2=a^2+2ab+b^2\leqslant|a|^2+2|a||b|+|b|^2=(|a|+|b|)^2.$$

但 $\sqrt{(a+b)^2}=|a+b|$，故上式平方根满足 $|a+b|\leqslant|a|+|b|$. 同理

$$|a-b|=|a+(-b)|\leqslant|a|+|-b|=|a|+|b|.$$

数学归纳法和良序原理

11.9 证明命题：前 n 个正整数的和是 $n(n+1)/2$；即

$$P(n):\quad 1+2+\cdots+n=\frac{1}{2}n(n+1).$$

证 ☞　当 $n=1$ 时性质成立，因为

$$P(1):\quad 1=\frac{1}{2}(1)(1+1).$$

设 $P(n)$ 成立，在 $P(n)$ 的两边同时加上 $n+1$ 得

$$\begin{aligned}1+2+3+\cdots+n+(n+1)&=\frac{1}{2}n(n+1)+(n+1)\\&=\frac{1}{2}[n(n+1)+2(n+1)]\\&=\frac{1}{2}[(n+1)(n+2)],\end{aligned}$$

即 $P(n+1)$ 成立. 也就是说，当 $P(n)$ 成立时，$P(n+1)$ 成立. 由数学归纳法 P 对于任何 $n\in\mathbf{N}$ 都成立.

11.10 证明命题 P:前 n 个正整数的平方和是 $n(n+1)(2n+1)/6$;即

$$P(n):\quad 1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

证 ☞ $P(1)$成立,因为

$$1^2=\frac{1(1+1)(2\cdot 1+1)}{6}.$$

假设 $P(n)$成立,在 $P(n)$两边同时加上$(n+1)^2$ 得

$$\begin{aligned}1^2+2^2+\cdots+n^2+(n+1)^2&=\frac{n(n+1)(2n+1)}{6}+(n+1)^2\\&=\frac{n(n+1)(2n+1)+6(n+1)^2}{6}\\&=\frac{(n+1)[n(2n+1)+6(n+1)]}{6}\\&=\frac{(n+1)(2n^2+7n+6)}{6}\\&=\frac{(n+1)(n+2)(2n+3)}{6}\\&=\frac{(n+1)[(n+1)+1][2(n+1)+1]}{6}.\end{aligned}$$

即 $P(n+1)$成立.因此当 $P(n)$成立时 $P(n+1)$成立,由数学归纳法,P 对所有的 $n\in\mathbf{N}$ 成立.

11.11 设 $a\neq1$,$n\geqslant1$ 时命题 P 为的定义如下

$$P(n):\quad 1+a+a^2+\cdots+a^n=\frac{a^{n+1}-1}{a-1}.$$

证明 P 对所有 n 成立.

证 ☞ $P(1)$成立,因为

$$1+a=\frac{a^2-1}{a-1}.$$

假设 $P(n)$成立,在 $P(n)$两边同时加上 a^{n+1}得

$$\begin{aligned}1+a+a^2+\cdots+a^n+a^{n+1}&=\frac{a^{n+1}-1}{a-1}+a^{n+1}\\&=\frac{a^{n+1}-1+(a-1)a^{n+1}}{a-1}\\&=\frac{a^{n+2}-1}{a-1}.\end{aligned}$$

即 $P(n+1)$成立.这样当 $P(n)$成立时,$P(n+1)$总成立.由数学归纳法,P 对所有的 $n\in\mathbf{N}$ 成立.

11.12 证明:如果 $n\in\mathbf{Z}$ 且 n 是正整数,那么 $n\geqslant1$(对有理数集 $\mathbf{Q}$ 不成立).换句话说,如果 $P(n)$表示命题 $n\geqslant1$,那么对于每一个 $n\in\mathbf{N}P(n)$成立.

证 ☞ 方法 1 (数学归纳法)

因为 $1\geqslant1$,当 $n=1$ 时 $P(n)$成立.设 $P(n)$成立,也就是说 $n\geqslant1$,在两边同时加 1 得

$$n+1\geqslant2>1.$$

即 $P(n+1)$成立.因此当 $P(n)$成立时 $P(n+1)$成立.由数学归纳法,P 对于每一个 $n\in\mathbf{N}$ 都成立.

方法 2 (良序原理)

设存在小于 1 的正整数,由良序原理得,存在最小的正整数 a 使得

$$0<a<1.$$

在不等式上乘以正整数 a 得

$$0<a^2<a.$$

因此,a^2 是一个小于 a 并且小于 1 的正整数,这与 a 是小于 1 的最小正整数矛盾,所以不存在小于 1 的正整数.

11.13 设 a,b 为正整数.证明:(a)如果 $b\neq1$,那么 $a<ab$.(b)如果 $ab=1$,那么 $a=1$ 且 $b=1$.(c)如果 n 是合数,那么 $n=ab$,$1<a,b<n$.

证 ☞ (a) 由问题 11.12,$b>1$.因此 $b-1>0$,也就是说 $b-1$ 是正的.由正整数 $\mathbf{N}$ 的性质[$\mathbf{P}_1$],下

面的积也是正的

$$a(b-1) = ab - a.$$

因此 $a<ab$，得证.

(b) 设 $b\neq 1$，由(a)，$a<ab=1$. 这与问题 11.12 矛盾. 所以 $b=1$，同理得 $a=1$.

(c) 如果 n 不是素数，那么有正因子 a 满足 $a\neq 1$ 且 $a\neq n$，那么 $n=ab$，$b\neq 1$ 且 $b\neq n$. 因此由问题 11.12 和(a)，$1<a,b<ab=n$.

11.14 证明定理 11.6(良序原理)：设 S 是一非空整数集，那么 S 含有一最小的元素.

证 ☞ 不妨设 S 无最小元素，设 M 是由那些小于 S 中每一个元素的整数构成的集合，那么 $1\in M$；否则，如果 $1\in S$，则 1 就是 S 中的最小元素. 设 $k\in M$，则 k 小于 S 中每一个元素，因此 $k+1\in M$；否则 $k+1$ 将成为 S 中的最小元素.

由数学归纳法，M 包含了所有的正整数，因此 S 是空集，这与假设 S 非空矛盾，所以原假设 S 无最小元素不成立，定理得证.

11.15 证明定理 11.5(第二数学归纳法)：设 P 是定义在整数 $n\geqslant 1$ 上的命题，满足：

(i) $P(1)$成立.

(ii) 对于所有的 $k(1\leqslant k<n)$当 $P(k)$成立时 $P(n)$成立，则 P 对所有的 $n\geqslant 1$ 成立.

证 ☞ 设 A 是 $P(n)$不成立的那些整数的集合，假设 A 非空，由良序原理，A 有最小元素 a_0. 由(i)，$a_0\neq 1$.

既然 a_0 是 A 的最小元素，则对任一整数 k. $(1\leqslant k<a_0)$，P 成立，由(ii)，对于 a_0，P 成立，这与 $a_0\in A$ 矛盾. 所以 A 是空集，P 对任意整数 $n\geqslant 1$ 成立.

带余除法

11.16 对于每一对整数 a 和 b，求整数 q 和 r，使得 $a=bq+r$ 且 $0\leqslant r<|b|$.

(a) $a=258, b=12$； (b) $a=573, b=-16$.

解 ☞ (a) 这里 a 和 b 是正的，b 除 a，即 258 被 12 除，如图 11-6(a)所示. 得 $q=21$，$r=6$.

(b) 这里 a 是正的，但 b 是负的，a 被 $|b|$ 除，即 573 除以 16，如图 11-6(b)所示，那么

$$573 = (16)(35) + 13 = 573 = (-16)(-35) + 13.$$

因此 $q=-35$ 且 $r=13$.

(a)	(b)	(c)	(d)
21	35	27	25
12)258	16)573	14)381	17)433
24	48	28	34
18	93	101	93
12	80	98	85
6	13	3	8

图 11-6

11.17 对于每一对整数 a 和 b，求整数 q 和 r，使得 $a=bq+r$ 且 $0\leqslant r<|b|$.

(a) $a=-381$, $b=14$；

(b) $a=-433$, $b=-17$.

解 ☞ 这里 a 在两种情况下都是负的，因此需作适当调整使 $0\leqslant r<|b|$.

(a) $|a|=381$ 被 $b=14$ 除，如图 11-6(c)所示，那么

$$381 = (14)(27) + 3. \quad 因此 \quad -381 = (14)(-27) - 3.$$

但 -3 是负的不能作为余数 r，于是，分别加和减 $b=14$ 得

$$-381 = (14)(-27) - 14 + 14 - 3 = (14)(-28) + 11.$$

故 $q=-28$，$r=11$.

(b) $|a|=433$ 被 $|b|=17$ 除，如图 11-6(d)所示，那么

$$433 = (17)(25) + 8, 因此 -433 = (-17)(25) - 8.$$

但 -8 是负的不能作为余数 r，通过分别加和减 $|b|=17$ 得

$$-433 = (-17)(25) - 17 + 17 - 8 = (-17)(26) + 9.$$

故 $q=26, r=9$.

11.18 证明下列命题：

(a) 任意整数 a 必有形式 $3k, 3k+1$ 或 $3k+2$.

(b) 三个连续的整数中必有一个是 3 的倍数.

证 ☞ (a) 由带余除法得

$$a = 3q + r, \quad 0 \leqslant r < 3.$$

由后一不等式知 $r=0, 1$ 或 2. 因此

$$a = 3q, \quad a = 3q+1, \text{或} a = 3q+2.$$

(b) 设三个连续整数是 $a, a+1$ 和 $a+2$. 由(a)得 $a=3k$ 或 $a=3k+1$ 或 $a=3k+2$. 如果 $a=3k$，那么 a 是 3 的倍数. 如果 $a=3k+1$，那么

$$a+2 = 3k+1+2 = 3(k+1).$$

因此 $a+2$ 是 3 的倍数. 如果 $a=3k+2$，那么

$$a+1 = 3k+2+1 = 3(k+1).$$

因此 $a+1$ 是 3 的倍数.

11.19 证明：$\sqrt{2}$不是有理数，即$\sqrt{2}\neq a/b$，a, b 为整数.

证 ☞ 设$\sqrt{2}$是有理数，则$\sqrt{2}=a/b$，a, b 为最简形式，即 $\gcd(a,b)=1$，上式两边同时平方得

$$2 = \frac{a^2}{b^2} \quad \text{或} \quad a^2 = 2b^2.$$

那么 2 整除 a^2. 既然 2 是素数，$2|b$. 因此 2 既整除 a 又整除 b，这与假设$\gcd(a,b)=1$ 矛盾，因此$\sqrt{2}$不是有理数.

11.20 证明定理 11.7(带余除法对于 a 和 b 为正整数的情形)：设 a, b 是正整数，证明存在非负整数 q 和 r 使得

$$a = bq + r \quad \text{且} \quad 0 \leqslant r < b. \qquad (*)$$

证 ☞ 如果 $a<b$，取 $q=0, r=a$. 如果 $a=b$，取 $q=1, r=0$. 在这两种情况中 q 和 r 满足(*).

对 a 用数学归纳法. 如果 $a=1$，那么 $a<b$ 或 $a=b$；因此，当 $a=1$ 时定理成立. 假设 $a>b$，那么 $a-b$ 是正的，且 $a-b<a$，由归纳假设得，定理满足 $a-b$. 因此存在 q' 和 r' 满足

$$a-b = bq'+r' \quad \text{且} \quad 0 \leqslant r' < b.$$

那么

$$a = bq'+b+r' = b(q'+1)+r'.$$

取 $q=q'+1$ 和 $r=r'$，那么 q 和 r 满足(*).

11.21 证明定理 11.7(带余除法)：设 a 和 b 是整数 $b\neq 0$，那么存在 q 和 r 使得

$$a = bq + r \quad \text{和} \quad 0 \leqslant r < |b|,$$

且 q 和 r 惟一.

证 ☞ 设 M 为对某些整数 x 的形如 $a-xb$ 的非负整数的集合. 如果 $x=-|a|b$，那么 $a-xb$ 是非负的(问题 11.78)；因此 M 非空，由良序原理，M 有一最小元素. 不妨设为 r. 因为 $r\in M$，我们有

$$r \geqslant 0 \quad \text{且} \quad r = a - qb,$$

对于某个整数 q. 我们只需要证明 $r<|b|$. 假设 $r\geqslant|b|$. 令 $r'=r-|b|$，那么 $r'\geqslant 0$ 且 $r'<r$，因为 $b\neq 0$. 进而

$$r' = r-|b| = a-qb-|b| = \begin{cases} a-(q+1)b, \text{如果 } b<0, \\ a-(q-1)b, \text{如果 } b>0. \end{cases}$$

在任一情况下，$r'\in M$. 这与 r 是 M 中最小元素矛盾. 因此 $r<|b|$，q 和 r 的存在性得证.

现在我们来证 q 和 r 的惟一性，设存在整数 q, r 和 q', r' 使得

$$a = bq + r \text{和} a = bq' + r' \quad \text{且} \quad 0 \leqslant r, r' < |b|.$$

那么 $bq+r=bq'+r'$；于是

$$b(q-q') = r' - r.$$

故 b 整除 $r'-r$. 但 $|r'-r|<|b|$，因为 $0\leqslant r, r'<|b|$. 因此 $r'-r=0$. 这意味着 $q-q'=0$，由于 $b\neq 0$. 所以 $r'=r, q'=q$，也就是说 q 和 r 是由 a, b 惟一决定的.

整除、素数和最大公因数

11.22 求下列各数所有的正因子：(a) 18，(b) $256=2^8$，(c) $392=2^3\cdot 7^2$.

解 ☞ (a) 由于 18 相对较小，我们简单地写下所有整除 18 的正整数，它们是

$$1,\ 2,\ 3,\ 6,\ 9,\ 18.$$

(b) 因为 2 是素数，所以 $256=2^8$ 的正因子，为 2 的不高于 8 的方幂，即

$$2^0,\ 2^1,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ 2^8.$$

换句话说 256 的正因子是：

$$1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128,\ 256.$$

(c) 因为 2 和 7 是素数 $392=2^3\cdot 7^2$ 的正因子就是 2 的不高于 3 的方幂乘 7 的不高于 2 的方幂，即

$$2^0\cdot 7^0,\ 2^1\cdot 7^0,\ 2^2\cdot 7^0,\ 2^3\cdot 7^0,\ 2^0\cdot 7^1,\ 2^1\cdot 7^1,\ 2^2\cdot 7^1,\ 2^3\cdot 7^1,$$
$$2^0\cdot 7^2,\ 2^1\cdot 7^2,\ 2^2\cdot 7^2,\ 2^3\cdot 7^2.$$

换句话说 392 的正因子是：

$$1,\ 2,\ 4,\ 8,\ 7,\ 14,\ 28,\ 56,\ 49,\ 98,\ 196,\ 392.$$

(这里使用了一般的结论：对于任何非零数 $n, n^0=1$)

11.23 列出 50 到 100 之间的所有素数.

解 ☞ 写出 50 到 100 之间除 1 和 p 两整数外，不能写成其他正整数乘积的整数，它们分别为

$$51,\ 53,\ 57,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 87,\ 89,\ 91,\ 93,\ 97.$$

11.24 设 $a=8316, b=10920$.

(a) 求 a,b 的最大公因子，$d=\gcd(a,b)$.

(b) 求整数 m 和 n，使得 $d=ma+nb$.

(c) 求 a,b 的最小公倍数，$\mathrm{lcm}(a,b)$.

解 ☞ (a)用较小的数 $a=8316$ 除较大的数 $b=10920$，然后反复用余数除除数直到余数为零，具体过程见图 11－7. 最后一个非零余数是 84，因此

$$84=\gcd(8316, 10920).$$

```
         1              3             5          6
8316)10920     2604)8316      504)2604     84)504
      8316           7812          2520        504
      2604            504            84          0
```

图 11－7

(b) 现在我们来求 m, n 便得

$$84=8316m+10920n.$$

图 11－7 中前三个商满足等式：

(1) $10920=1(8316)+2604$，　$2604=10920-1(8316)$.

(2) $8316=3(2604)+504$，　$504=8316-3(2604)$.

(3) $2604=5(504)+84$，　$84=2604-5(504)$.

等式(3)指出 84 是 2604 和 504 的线性组合，用(2)式代替(3)中的 504，可以将 84 写成 2604 与 8316 的线性组合如下：

(4) $84=2604-5(8316-3(2604))=2604-5(8316)+15(2604)$
$\quad=16(2604)-5(8316)$.

用(1)式代替(4)式中的 2604，可以将 84 写成 8316 和 10920 的线性组合如下：

$$\begin{aligned}84&=16(10920-1(8316))-5(8316)\\&=16(10920)-16(8316)-5(8316)\\&=-21(8316)+16(10920).\end{aligned}$$

这就是要求的线性关系，所以 $m=-21, n=16$.

(c) 由定理 11.15.

$$\mathrm{lcm}(a,b)=\frac{|ab|}{\gcd(a,b)}=\frac{(8316)(10920)}{84}=1081080.$$

11.25 设 $a=37, b=249$. (a) 求 $d=\gcd(a,b)$. (b) 求整数 m 和 n，使得 $d=ma+nb$. (c) 求 $\operatorname{lcm}(a,b)$.

解 (a) 用较小的数 $a=37$ 除较大的数 $b=249$，然后反复用余数去除除数直到余数为 0，具体过程如图 11-8 所示. 最后一个非零余数为 1，因此

$$1=\gcd(37,249)$$

$$\begin{array}{r} 6 \\ 37\overline{)249} \\ 222 \\ \hline 27 \end{array} \quad \begin{array}{r} 1 \\ 27\overline{)37} \\ 27 \\ \hline 10 \end{array} \quad \begin{array}{r} 2 \\ 10\overline{)27} \\ 20 \\ \hline 7 \end{array} \quad \begin{array}{r} 1 \\ 7\overline{)10} \\ 7 \\ \hline 3 \end{array} \quad \begin{array}{r} 2 \\ 3\overline{)7} \\ 6 \\ \hline 1 \end{array} \quad \begin{array}{r} 3 \\ 1\overline{)3} \\ 3 \\ \hline 0 \end{array}$$

图 11-8

(b) 现在求 m 和 n 使得

$$1=37m+249n.$$

图 11-8(除最后一个)的商满足下面 5 个等式：

(1) $27=249-6(37)$.

(2) $10=37-1(27)$.

(3) $7=27-2(10)$.

(4) $3=10-1(7)$.

(5) $1=7-2(3)$.

用(4)和(5)将 1 写成 7 和 10 的线性组合如下：

(6) $1=7-2(10-1(7))=7-2(10)+2(7)=3(7)-2(10)$.

用(6)和(3)将 1 写成 10 和 27 的线性组合如下：

(7) $1=3(27-2(10))-2(10)=3(27)-6(10)-2(10)=3(27)-8(10)$.

用(7)和(2)将写成 27 和 37 的线性组合如下：

(8) $1=3(27)-8(37-1(27))=3(27)-8(37)+8(27)=11(27)-8(37)$.

用(8)和(1)将 1 写成 37 和 249 的线性组合如下：

$$1=11(249-6(37))-8(37)=11(249)-66(37)-8(37)=-74(37)+11(249)$$

这就是要求的线性组合，所以 $m=-74\quad n=11$.

(c) 由定理 11.15，

$$\operatorname{lcm}(a,b)=\frac{|ab|}{\gcd(a,b)}=\frac{(37)(249)}{1}=9213.$$

11.26 求下列各数的惟一分解式：

(a) 135；(b) 1330；(c) 3105；(d) 211.

解 (a) $135=5\cdot 27=5\cdot 3\cdot 3\cdot 3$ 或 $135=3^3\cdot 5$.

(b) $1330=2\cdot 665=2\cdot 5\cdot 133=2\cdot 5\cdot 7\cdot 19$.

(c) $3105=5\cdot 621=5\cdot 3\cdot 207=5\cdot 3\cdot 3\cdot 69=5\cdot 3\cdot 3\cdot 3\cdot 23$ 或 $3105=3^3\cdot 5\cdot 23$.

(d) 素数 2,3,5,7,11,13 中没有一个整除 211；因此 211 不能分解，也就是说 211 是素数.（注：只需尝试小于 $\sqrt{211}$ 的素数）

11.27 设 $a=2^5\cdot 3^5\cdot 5^4\cdot 11^6\cdot 17^3$, $b=2^5\cdot 5^3\cdot 7^2\cdot 11^4\cdot 13^2$，求 $\gcd(a,b)$ 和 $\operatorname{lcm}(a,b)$.

解 那些在 a 和 b 中都出现的素数 p_i 也会出现在 $\gcd(a,b)$ 中，进一步说，$\gcd(a,b)$ 中 p_i 的系数取 a,b 中 p_i 系数较小的一个，因此

$$\gcd(a,b)=2^3\cdot 5^3\cdot 11^4.$$

那些在 a 或 b 中出现的素数 p_i 也会出现在 $\operatorname{lcm}(a,b)$，$\operatorname{lcm}(a,b)$ 中，p_i 的系数取 a,b 中 p_i 系数较大的一个，因此

$$\operatorname{lcm}(a,b)=2^5\cdot 3^5\cdot 5^4\cdot 7^2\cdot 11^6\cdot 13^2\cdot 17^3.$$

11.28 证明定理 11.8：设 a,b,c 是整数，

(i) 如果 $a|b, b|c$，那么 $a|c$.

(ii) 如果 $a|b$，那么对于任意整数 x，$a|bx$.

(iii) 如果 $a|b, a|c$，那么 $a|(b+c)$，$a|(b-c)$.

(iv) 如果 $a|b$ 且 $b\neq 0$,那么 $a=\pm b$ 或 $|a|<|b|$.

(v) 如果 $a|b,b|a$,那么 $|a|=|b|$ 即 $a=\pm b$.

(vi) 如果 $a|1$,那么 $a=\pm 1$.

证 (i) 如果 $a|b,b|c$,那么存在 x 和 y 使得 $ax=b,by=c$. 用 ax 代替 b 我们得到 $axy=c$,因此 $a|c$.

(ii) 如果 $a|b$,那么存在一个整数 c 使得 $ac=b$,在此式两边同乘以 x,得 $acx=bx$,因此 $a|bx$.

(iii) 如果 $a|b,a|c$,那么存在 x,y 使得 $ax=b,ay=c$. 将两式相加,得到

$$ax+ay=b+c,\quad a(x+y)=b+c.$$

因此 $a|(b+c)$. 将两式相减得

$$ax-ay=b-c,\quad a(x-y)=b-c.$$

因此 $a|(b-c)$.

(iv) 如果 $a|b$,那么存在 c 使得 $ac=b$. 那么

$$|b|=|ac|=|a||c|.$$

由问题 11.12(b),$|c|=1$ 或 $|a|<|a||c|=|b|$. 如果 $|c|=1$,那么 $c=\pm 1$;即 $a=\pm b$,所以得证.

(v) 如果 $a|b$,那么 $a=\pm b$ 或 $|a|<|b|$;如果 $|a|<|b|$,$b\nmid a$,因此 $a=\pm b$.

(vi) 如果 $a|1$,那么 $a=\pm 1$ 或 $|a|<|1|=1$,由问题 11.12(a),$|a|\geqslant 1$,因此 $a=\pm 1$.

11.29 $\mathbf{Z}$ 的一个非空子集 J 称为一个*理想*,如果 J 有下面两个性质:

(1) 如果 $a,b\in J$,那么 $a+b\in J$.

(2) 如果 $a\in J$ 且 $n\in Z$,那么 $na\in J$.

设 d 是一个理想 $J\neq\{0\}$ 的最小的正整数,证明 d 整除 J 中每一个元素.

证 由于 $J\neq\{0\}$,存在 $a\in J$ 且 $a\neq 0$,那么 $-a=(-1)a\in J$,因此 J 含有正的元素. 由良序原理,J 含有最小的正整数,所以 d 存在,现设 $b\in J$,b 被 d 除,由带余除法存在 q 和 r 使得

$$b=qd+r,\quad 0\leqslant r<d.$$

现 $b,d\in J$,J 是一理想,因此 $b+(-q)d=r$ 也属于 J. 由 d 的最小性,我们得 $r=0$. 故 $d|b$ 命题得证.

11.30 证明定理 11.12:设 d 是形如 $ax+by$ 的最小正整数,那么 $d=\gcd(a,b)$.

证 考虑集合 $J=\{ax+yb:x,y\in z\}$,那么

$$a=1(a)+0(b)\in J,b=0(a)+1(b)\in J.$$

又设 $s,t\in J$,到 $s=x_1a+y_1b,t=x_2a+y_2b$,那么对于任意整数 $n\in\mathbf{Z}$,

$$s+t=(x_1+x_2)a+(y_1+y_2)b,\quad ns=(nx_1)a+(ny_1)b$$

也属于 J. 因此 J 是一理想,设 d 是 J 中最小的正整数,我们说 $d=\gcd(a,b)$.

由问题 11.28,d 整除 J 中每一个元素,特别地 $d|a,d|b$. 现设 h 既整除 a 又整除 b,则对于任意 x 和 yh 整除 $xa+yb$:也就是说 h 整除 J 中的每一个元素,因此 h 整除 d,$h<d$,故 $d=\gcd(a,b)$.

11.31 证明定理 11.16:设 $\gcd(a,b)=1$,a 和 b 都整除 c,那么 ab 整除 c.

证 由 $\gcd(a,b)=1$ 存在 x 和 y 使得 $ax+by=1$. 因为 $a|c,b|c$ 存在 m 和 n 使得 $c=ma$ 和 $c=nb$. 在 $ax+by=1$ 上乘以 c 得

$$acx+bcy=c \text{ 或 } a(nb)x+b(ma)y=c \text{ 或 } ab(nx\pm my)=c.$$

因此 ab 整除 c.

11.32 证明推论 11.18:设素数 p 整除积 ab,那么 $p|a$ 或 $p|b$.

证 设 p 不整除 a,那么 $\gcd(p,a)=1$,因为 p 的因子仅有 ± 1 和 $\pm p$. 故存在整数 m 和 n 使得 $1=mp+na$,在等式上乘以 b 得 $b=mpb+nab$. 由假设 $p|ab$,若设 $ab=cp$ 则

$$b=mpb+nab=mpb+ncp=p(mb+nc).$$

因此 $p|b$,命题得证.

11.33 证明:(a) 设 $p|q$,p 和 q 互素,那么 $p=q$;(b) 设 $p|q_1q_2\cdots q_r$,p 和 q_i 互素,那么 p 一定等于某个 q_i.

证 (a) q 的因子仅有 ± 1 和 $\pm q$,因为 $p>1$,$p=q$.

(b) 如果 $r=1$,那么由(a),$p=q_1$. 设 $r>1$,由问题 11.32(推论 11.18),$p|q_1$,或 $p|(q_2\cdots q_r)$,如果

$p|q_1$，那么由(a)，$p=q_1$，否则 $p|(q_2\cdots q_r)$. 重复上述证明，即得 $p=q_2$，或 $p|(q_3\cdots q_r)$，最终(或由归纳法)p 一定等于某个 q_i.

11.34 证明算术基本定理(定理 11.19)：每一个整数 $n(>1)$都可以(不考虑顺序)惟一地分解成素数积.

证 ☞ 我们已经证明了定理 11.10，即这样的素数积存在. 因此只需证明这一分解的惟一性(不考虑顺序). 假设

$$n = p_1p_2\cdots p_k = q_1q_2\cdots q_r.$$

其中 p_i 和 q_j 都是素数. 由上式知 $p_1|(q_1\cdots q_r)$，故由问题 11.33，p_1 一定等于某个 q_j. 我们重排一下使得 $q_1=p_1$，那么

$$p_1p_2\cdots p_k = p_1q_2\cdots q_r \quad 即 \quad p_2\cdots p_k = q_2\cdots q_r.$$

由同样的证明，可以重排使得 $p_2=q_2$，等等. 因此 n 可以惟一地写成素数积(不考虑顺序).

同余

11.35 判断下列各式的正误.

(a) $446\equiv278(\text{mod }7)$.　(b) $793\equiv682(\text{mod }9)$.

(c) $269\equiv413(\text{mod }12)$.　(d) $473\equiv369(\text{mod }26)$.

(e) $445\equiv536(\text{mod }18)$.　(f) $383\equiv126(\text{mod }15)$.

解 ☞ 回顾 $a\equiv b(\text{mod}m)$当且仅当 m 整除 $a-b$.

(a) **方法 1** 求差 $446-278=168$. 用模 $m=7$ 除差 168 余数是 0，因此本题正确.

方法 2 在等式两边都模 7 化简. 用 7 除 446 余数是 $r=5$，用 7 除 278 余数也是 $r=5$，因此 $446\equiv278$ (mod7).

(b) 用模 $m=9$ 除差 $793-682=111$，余数不是 0，因此本题错误(或者用 9 除 793 得余数 $r=1$，但是 9 除 682 得余数为 $r=6$).

(c) 正确，因为 12 整除 $269-413=-144$.

(d) 正确，因为 26 整除 $472-369=104$.

(e) 错误，因为 18 不能整除 $445-536=-91$.

(f) 错误，因为 15 不能整除 $383-126=157$.

11.36 求模 8 与下列各数同余的最小非负整数.

(a) 379；(b) 695；(c) -578；(d) -285(该整数应属于集合{0，1，2，…，7}.)

解 ☞ (a) 用 $m=8$ 除 379 得余数 3，因此

$$379\equiv 3(\text{mod }8).$$

(b) 用 $m=8$ 除 695 得余数 7，因此

$$695\equiv 7(\text{mod }8).$$

(c) 用 $m=8$ 除 578 得余数 2，因此

$$-578\equiv-2\equiv 6(\text{mod }8).$$

(我们通过在-2 上加模 $m=8$ 得到 6)

(d) 用 $m=8$ 除 285 得余数 5，因此

$$-285\equiv-5\equiv 3(\text{mod }8).$$

11.37 求模 7 分别与下列各数同余的绝对值最小的整数：

(a) 386；(b) 257；(c) -192；(d) -466.

(所求整数应在集合{-3，-2，-1，0，1，2，3}中)

解 ☞ (a) 用 $m=7$ 除 386 余数为 1；因此

$$386\equiv 1(\text{mod }7).$$

(b) 用 $m=7$ 除 257 余数为 5；因此

$$257\equiv 5\equiv-2(\text{mod }7).$$

(由在 5 上减去模 $m=7$ 得到-2)

(c) 用 $m=7$ 除 192 余数为 3；因此

$$-192 \equiv -3 \pmod 7).$$

(d) 由 $m=7$ 除 466 余数为 4;因此

$$-466 \equiv -4 \equiv 3 \pmod 7).$$

(由在 −4 上加上模 7 得到 3)

11.38 求 1 到 100 之间的所有模 $m=13$ 余 6 的整数. 也就说求所有的 x,$1 \leqslant x \leqslant 100$ 便得

$$x \equiv 6 \pmod{13}.$$

解 ☞ 依次将模 $m=13$ 的倍数加到 6 上得:

$$6+0=6,\quad 6+13=19,\quad 19+13=32,\quad 32+13=45,$$
$$45+13=58,\quad 58+13=71,\quad 71+13=84,\quad 84+13=97.$$

也就是

$$6, 19, 32, 45, 58, 71, 84, 97.$$

11.39 求 −50 与 50 之间的所有模 12 余 21 的整数,也就是求 x,$-50 \leqslant x \leqslant 50$ 且满足

$$x \equiv 21 \pmod{12}.$$

在 21 上加减模 12 的倍数得:

$$21+0=21,\quad 21-12=33,\quad 33+12=45,\quad 21-12=9,$$
$$9-12=-3,\quad -3-12=-15,\quad -15-12=-27,\quad -27-12=-39.$$

也就是说

$$-39, -27, -15, -3, 9, 21, 33, 45.$$

11.40 证明定理 11.20:设 m 是一正整数,那么:

(i) 对于任一整数 a,我们有 $a \equiv a \pmod m$.

(ii) 如果 $a \equiv b \pmod m$,那么 $b \equiv a \pmod m$.

(iii) 如果 $a \equiv b \pmod m$,$b \equiv c \pmod m$,那么 $a \equiv c \pmod m$.

证 ☞ (i) 差 $a-a=0$ 被 m 整除,因此 $a \equiv a \pmod m$.

(ii) 如果 $a \equiv b \pmod m$,那么 $m \mid (a-b)$,所以 m 整除 $-(a-b)=b-a$. 因此,$b \equiv a \pmod m$.

(iii) 由题设得 $m \mid (a-b)$,$m \mid (b-c)$. 所以 m 整除和 $(a-b)+(b-c)=a-c$,因此,$a \equiv c \pmod m$.

11.41 证明定理 11.21:设 $a \equiv c \pmod m$,$b \equiv d \pmod m$,那么:

(i) $a+b \equiv c+d \pmod m$.

(ii) $a \cdot b \equiv c \cdot d \pmod m$.

证 ☞ 由题设得 $m \mid (a-c)$,$m \mid (b-d)$.

(i) 那么 m 整除和 $(a-c)+(b-d)=(a+b)-(c+d)$,因此

$$a+b \equiv c+d \pmod m.$$

(ii) 那么 m 整除积 $b(a-c)=ab-bc$ 与积 $c(b-d)=bc-cd$,这样 m 就整除和

$$(ab-bc)+(bc-cd)=ab-cd.$$

因此 $ab \equiv cd \pmod m$.

11.42 证明:如果 $a+b \equiv a+c \pmod m$,那么 $b \equiv c \pmod m$.

(也就是说模 m 满足加法消去律)

证 ☞ 根据假设,m 整除差 $(a+b)-(a+c)=b-c$,所以 $b \equiv c \pmod m$,命题得证.

11.43 设 $d=\gcd(a,b)$,证明 a/d 和 b/d 互素.

证 ☞ 存在 x 和 y 使得 $d=xa+yb$. 在等式两边同除 d,得 $1=x(a/d)+y(b/d)$. 因此 a/d 和 b/d 互素.

11.44 证明定理 11.23:设 $ab \equiv ac \pmod m$,且 $d=\gcd(a,m)$,那么 $b \equiv c \pmod{m/d}$.

证 ☞ 由假设,m 整除 $ab-ac=a(b-c)$,故存在 x 满足 $a(b-c)=mx$. 在等式两边同除 d 得

$$(a/d)(b-c)=(m/d)x.$$

因此 m/d 整除 $(a/d)(b-c)$. 因 m/d 和 a/d 互素,m/d 整除 $b-c$,即 $b \equiv c \pmod{m/d}$,命题得证.

剩余类和欧拉函数$\varnothing$

11.45 分别写出下列模 m 的完全剩余系，一个由最小的非负整数组成，另一个由绝对值最小的整数组成：

$$(a)\ m=9;\qquad (b)\ m=12.$$

解 ☞ 第一种情况中取$\{0,1,2,\cdots,m-1\}$，另一种情况取$\{-(m-1)/2,\cdots,-1,0,1,\cdots,(m-1)/2\}$或$\{-(m-2)/2,\cdots,-1,0,1,\cdots,m/2\}$.

根据 m 的奇偶性：

(a) $\{0,1,2,3,4,5,6,7,8\}$和$\{-4,-3,-2,-1,0,1,2,3,4\}$.

(b) $\{0,1,2,3,4,5,6,7,8,9,10,11\}$和$\{-5,-4,-3,-2,-1,0,1,2,3,4,5,6\}$.

11.46 求下列模 m 的简化剩余系和$\varnothing(m)$：(a) $m=9$；(b) $m=12$；(c) $m=13$；(d) $m=16$.

解 ☞ 选取小于 m 并且与 m 互素的正整数，这些数的个数是$\varnothing(m)$.

(a) $\{1,2,4,5,7,8\}$；因此$\varnothing(9)=6$.

(b) $\{1,5,7,11\}$；因此$\varnothing(12)=4$.

(c) $\{1,2,3,4,5,6,7,8,9,10,11,12\}$；因此$\varnothing(13)=12$.

(d) $\{1,3,5,7,9,11,13,15\}$；因此$\varnothing(16)=8$.

11.47 回顾 $S_m=\{0,1,2,\cdots,m-1\}$是一个模 m 完全剩余系，证明：

(a) 任意 m 个连续的整数都是一个模 m 完全剩余系.

(b) 如果 $\gcd(a,m)=1$，那么 $aS_m=\{0,a,2a,3a,\cdots,(m-1)a\}$是模 m 的一个完全剩余系.

证 ☞ (a)考虑任意连续的 m 个整数，如

$$\{a,a+1,a+2,\cdots,a+(m-1)\}.$$

它们中任意两个的差 s 都小于 m，因此 m 不能整除 s，故这些整数模 m 不同余，命题得证.

(b) 设 $ax\equiv ay(\bmod m)$，$x,y\in S_m$. 由 $\gcd(a,m)=1$ 及修正消去律定理 11.23 知 $x\equiv y(\bmod m)$. 因为 $x,y\in S_m$，得 $x=y$. 即 aS_m 是模 m 的一个完全剩余系.

11.48 求一由 3 的倍数组成的模 $m=8$ 的完全剩余系.

解 ☞ 由问题 11.47(b)，$3S_8=\{0,3,6,9,12,15,18,21\}$是模 8 的一个完全剩余系.

11.49 证明：如果 p 是素数，那么

$$\varnothing(p^n)=p^n-p^{n-1}=p^{n-1}(p-1).$$

证 ☞ 显然，$\gcd(a,p^n)\neq1$ 当且仅当 p 整除 a，这样在 1 与 p^n 之间与 p^n 不互素的数是 p 的倍数，即

$$p,\quad 2p,\quad 3p,\quad \cdots,\quad p^{n-1}(p).$$

一共有 p^{n-1}个这样的 p 的倍数. 其他的所有 1 到 p^n 间的数都与 p^n 互素，因此

$$\varnothing(p^n)=p^n-p^{n-1}=p^{n-1}(p-1).$$

得证.

11.50 求：(a) $\varnothing(81)$，$\varnothing(125)$，$\varnothing(7^6)$；(b)$\varnothing(72)$，$\varnothing(3000)$.

解 ☞ (a) 由问题 11.49，

$$\varnothing(81)=\varnothing(3^4)=3^3(3-1)=27(2)=54.$$
$$\varnothing(125)=\varnothing(5^3)=5^2(5-1)=25(4)=100.$$
$$\varnothing(7^6)=7^5(7-1)=6(7^5).$$

(b) 由定理 11.24 知$\varnothing$是可乘的，

$$\varnothing(72)=\varnothing(3^2\cdot2^3)=\varnothing(3^2)\varnothing(2^3)=3(3-1)\cdot2^2(2-1)=24.$$
$$\varnothing(3000)=\varnothing(3\cdot2^2\cdot5^3)=\varnothing(3)\varnothing(2^2)\varnothing(5^3)=2\cdot2\cdot5^2(5-1)=400.$$

11.51 证明定理 11.24：如果 a,b 互素，那么$\varnothing(ab)=\varnothing(a)\varnothing(b)$.

证 ☞ 设 a 和 b 是互素的正整数，设 S 是从 1 到 ab 的整数的集合，排列如图11-9，即 S 的第一排是 1 到 a，第二排是 $a+1$ 到 $2a$，等等. 既然 a 与 b 互素，任意整数 x 与 ab 互素当且仅当 x 既和 a 互

素又与 b 互素. 我们求 S 的排列中这样的整数.

因为 $na+k\equiv k \pmod a$，所以 S 中的每一列都属于模 a 的同一个剩余类，因此 S 中任一整数 x 与 a 互素当且仅当 x 属于以 k 开头的列，且 k 和 a 互素，因此由于第一行是模 a 的剩余类，故有 $\varnothing(a)$ 个这样的列.

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & k & \cdots & a \\ a+1 & a+2 & a+3 & \cdots & a+k & \cdots & 2a \\ 2a+1 & 2a+2 & 2a+3 & \cdots & 2a+k & \cdots & 3a \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & & (b-1)a+k & \cdots & ba \end{array}$$

图 11 - 9

现在我们考虑 S 中由下列数构成的任一个列

$$k,\quad a+k,\quad 2a+k,\quad 3a+k,\quad (b-1)a+k. \qquad (*)$$

我们说，这些 b 整数来自模 b 的一个剩余系，也就是说，这些数中无两个模 b 同余，设

$$na+k\equiv n'a+k \pmod b \quad 即 \quad na\equiv n'a \pmod b).$$

但 a 和 b 互素，由修正消去律

$$n\equiv n' \pmod b).$$

但 n 和 n' 属于 $\{0,1,2,\cdots,b-1\}$，故 $n=n'$ 从而 $(*)$ 是模 b 的一个完全剩余系，因此 $(*)$ 含有 $\varnothing(b)$ 个与 b 互素的整数.

我们已经证明了 S 中含有 $\varnothing(a)$ 列与 a 互素的数，并且每一列都有 $\varnothing(b)$ 个与 b 互素的数. 于是有 $\varnothing(a)\varnothing(b)$ 个整数既和 a 又和 b 互素，即和 ab 互素. 所以

$$\varnothing(ab)=\varnothing(a)\varnothing(b).$$

得证.

模 m 的运算和 $\mathbf{Z}_m$

11.52 写出(a)和(b)的加法表和乘法表：(a) $\mathbf{Z}_4$；(b) $\mathbf{Z}_7$.

解 ☞ (a) 见图 11 - 10；(b) 见图 11 - 11.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

图 11 - 10

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

图 11 - 11

11.53 在 $\mathbf{Z}_{11}$ 中，求：(a) $-2,-3,-5,-8,-9,-10$；(b) $2/7, 3/7, 5/7, 8/7, 10/7, 1/7$.

解 ☞ (a) 由 $(m-a)+a=0$ 得，$-a=m-a$. 因此：

$$-2=11-2=9,\quad -5=11-5=6,\quad -9=11-9=2,$$

$$-3=11-3=8,\quad -8=11-8=3,\quad -10=11-10=1.$$

(b) 由 a/b 的定义，即整数 c，使得 $bc=a$ 成立. 由于我们要除 7，故写出 7 的乘法表，即

×	0	1	2	3	4	5	6	7	8	9	10
7	0	7	3	10	6	2	9	5	1	8	4

我们来求表中的数，答案就在这些数中，因此

$$2/7=5,\quad 3/7=2,\quad 5/7=7,\quad 8/7=9,\quad 10/7=3,\quad 1/7=8.$$

(注意 $7^{-1}=8$，因为 $7(8)=8(7)=1$).

11.54　设 p 为素数，在 $\mathbf{Z}_p$ 中证明：

(a) 如果 $ab=ac$ 且 $a\neq 0$，那么 $b=c$.

(b) 如果 $ab=0$，那么 $a=0$ 或 $b=0$.

证 (a) 如果在 $\mathbf{Z}_p$ 中 $ab=ac$，那么 $ab\equiv ac(\bmod p)$，由 $a\neq 0$，$\gcd(p,a)=1$ 及定理 11.22，可以消去 a 得到

$$b\equiv c(\bmod p).$$

因此在 $\mathbf{Z}_p$ 中 $b=c$.

(b) 如果在 $\mathbf{Z}_p$ 中 $ab=0$，那么 $ab\equiv 0(\bmod p)$，因此 p 整除积 ab，又因为 p 是素数，$p|a$ 或 $p|b$；即

$$a\equiv 0(\bmod p)\quad 或\quad b\equiv 0(\bmod p).$$

所以在 $\mathbf{Z}_p$ 中 $a=0$ 或 $b=0$.

11.55　设 $\gcd(a,m)=1$，证明 a 在 $\mathbf{Z}_m$ 中有一乘法逆元.

证 因为 $a\neq 0$ 且 $\gcd(a,m)=1$，故存在 x 和 y，使得 $ax+my=1$，或写成 $ax-1=my$，所以 m 整除 $ax-1$ 即 $ax\equiv 1(\bmod m)$. 将 x 模 m 化简成 $\mathbf{Z}_m$ 中的元素 x'，那么 $ax'=1$ 在 $\mathbf{Z}_m$ 中.

11.56　在 $\mathbf{Z}_m$ 中求 a^{-1}. (a) $a=37$　$m=249$；(b) $a=15$　$m=234$.

解 (a) 求 $d=\gcd(37,249)$，仿照问题 11.25. 因为 $d=\gcd(37,249)=1$，所以 a^{-1} 存在. 求整数 x 和 y 使得 $37x+249y=1$. 由问题 11.25 知

$$-74(37)+11(249)=1,\quad -74(37)\equiv 1(\bmod 249).$$

把 $m=249$ 加到 -74 上得 $-74+249=175$，因此

$$(175)(37)\equiv 1(\bmod 249).$$

因此 $a^{-1}=175$ 在 $\mathbf{Z}_{249}$ 中.

(b) 求 $d=\gcd(15,234)=3$，由于 $d\neq 1$，15 在 $\mathbf{Z}_{234}$ 中无乘法逆元.

11.57　考虑下列 $\mathbf{Z}_7$ 上的多项式：

$$f(x)=6x^3-5x^2+2x-4,\quad g(x)=5x^3+2x^2+6x-1,$$
$$h(x)=3x^2-2x-5.$$

求：(a) $f(x)+g(x)$；　(b) $f(x)h(x)$.

证 先在整数 Z 上进行上述运算，然后将其系数模 7 化简.

(a) 我们有

$$\begin{array}{r} 6x^3-5x^2+2x-4\\ \underline{5x^3+2x^2+6x-1}\\ 11x^3-3x^2+8x-5\end{array}\quad 或\quad 4x^3-3x^2+x-5\quad 或\quad 4x^3+4x^2+x+2.$$

(b) 我们有

$$\begin{array}{rrrrrr} & & 6x^3 & -5x^2 & +2x & -4\\ & & & \underline{3x^2} & \underline{-2x} & \underline{-5}\\ 18x^5 & -15x^4 & +6x^3 & -12x^2 & & \\ & -12x^4 & +10x^3 & -4x^2 & +8x & \\ & & -30x^3 & +25x^2 & -10x & +20\\ \hline 18x^5 & -27x^4 & -14x^3 & +9x^2 & -2x & +20 \end{array}$$

或 $4x^5-6x^4\qquad +2x^2-2x+6$

或 $4x^5+x^4+2x^2+5x-6$

同余方程

11.58 解同余方程 $f(x)=4x^4-3x^3+2x^2+5x-4\equiv 0 \pmod 6$.

解 由于这个方程是非线性的，由一一检验模 6 的完全剩余系中的数的方法求解. 模 6 的一个完全剩余系如下

$$\{0,1,2,3,4,5\}$$

我们有

$$f(0)=-4\not\equiv 0 \pmod 6.$$
$$f(1)=4-3+2+5-4=4\not\equiv 0 \pmod 6.$$
$$f(2)=64-24+8+10-4=54\equiv 0 \pmod 6.$$
$$f(3)=324-81+18+15-4=272\equiv 2\not\equiv 0 \pmod 6.$$
$$f(4)=1024-192+32+20-4=880\equiv 4\not\equiv 0 \pmod 6.$$
$$f(5)=2500-375+50+25-4=2196\equiv 0 \pmod 6.$$

因此只有 2 和 5 是 $f(x)$ 模 6 的根，即$\{2,5\}$是一个完整的解集合.

11.59 解同余方程

$$f(x)=26x^4-31x^3+46x^2-76x+57\equiv 0 \pmod 8.$$

解 首先，我们模 8 化简 $f(x)$ 的系数，得到等价的同余方程

$$g(x)=2x^4-7x^3+6x^2-4x+1\equiv 0 \pmod 8.$$

由于 $7\equiv -1 \pmod 8$，$6\equiv -2 \pmod 8$，可以进一步简化原方程得同余方程

$$h(x)=2x^4+x^3-2x^2-4x+1\equiv 0 \pmod 8.$$

检验模 8 的一个完全剩余系，为了运算方便选择下面一个完全剩余系

$$\{-3,-2,-1,0,1,2,3,4\}.$$

（即选择绝对值最小的组数组成的完全剩余系）把这些数代入 $h(x)$ 得

$$h(-3)=130\equiv 2 \pmod 8,\quad h(1)=-2\equiv 6 \pmod 8,$$
$$h(-2)=25\equiv 1 \pmod 8,\quad h(2)=25\equiv 1 \pmod 8,$$
$$h(-1)=94\equiv 6 \pmod 8,\quad h(3)=160\equiv 0 \pmod 8,$$
$$h(0)=91\equiv 3 \pmod 8,\quad h(4)=513\equiv 1 \pmod 8,$$

因此，3 是 $f(x) \pmod 8$ 的惟一解.

11.60 解下列线性同余方程：

(a) $3x\equiv 2 \pmod 8$；(b) $6x\equiv 5 \pmod 9$；(c) $4x\equiv 6 \pmod{10}$.

解 由于模相对较小，由一一尝试的方法来解. 回顾 $ax\equiv b \pmod m$，恰好有 $d=\gcd(a,m)$ 个解，如果 d 能整除 b.

(a) 这里 $\gcd(3,8)=1$，于是方程有惟一解，检验 $0,1,2,\cdots,7$，得

$$3(6)=18\equiv 2 \pmod 8.$$

(b) 这里 $\gcd(6,9)=3$，但 3 不整除 5，于是方程无解.

(c) 这里 $\gcd(4,10)=2$，2 整除 6，于是方程有两个解.

方法一 检验 $0,1,2,3,\cdots,9$，得

$$4(4)=16\equiv 6 \pmod{10},$$
$$4(9)=36\equiv 6 \pmod{10}.$$

因此 4 和 9 是方程的解.

方法二 在方程两边和模上同除以 $\gcd(4,10)=2$，得同余方程

$$2x\equiv 3 \pmod 5.$$

此方程有惟一解 $x=4$，即为原方程的解. 在这个解上加上新的模 5，得

$$x=4+5=9$$

是原方程的第二个解，因此 4 和 9 是我们所要求的两个解.

11.61 解同余方程 $1092x\equiv 213 \pmod{2295}$.

解 因为模 $m=2295$ 相对较大，所以不宜用一一尝试的方法. 首先用带余除法求 $d=\gcd$

$(1092,2295)=3$. 213 被 $d=3$ 除，得余数 0. 即 3 整除 213，因此方程有 3 个解(不同余).

模和方程同除以 3，得同余方程

$$364x \equiv 71 \pmod{765}. \qquad (*)$$

由于被 $d=\gcd(1092,2295)=3$ 除，故 364 和 765 互素，所以方程$(*)$模 765 有惟一解. 先求$(**)$的解，再求$(*)$的解.

$$364x \equiv 1 \pmod{765}. \qquad (**)$$

它的解可以通过求 s 和 t 使 $364s+765t=1$ 求得. s 和 t 的求解可用带余除法(如问题 11.25).

用 $a=364$ 去除 $m=765$，反复用余数去除除数直到余数为零，如图 11-12. 得到下面四个等式：

(1) $37=765-2(364)$.

(2) $31=364-9(37)$.

(3) $6=37-1(31)$.

(4) $1=31-5(6)$.

$$\begin{array}{r} 2 \\ 364\overline{)765} \\ 728 \\ \hline 37 \end{array} \qquad \begin{array}{r} 9 \\ 37\overline{)364} \\ 333 \\ \hline 31 \end{array} \qquad \begin{array}{r} 1 \\ 31\overline{)37} \\ 31 \\ \hline 6 \end{array} \qquad \begin{array}{r} 5 \\ 6\overline{)31} \\ 30 \\ \hline 1 \end{array}$$

图 11-12

用(4)和(3)将 1 写成 31 和 37 的线性组合

(5) $1=31-5[37-1(31)]=6(31)-5(37)$.

用(5)和(2)将 1 写成 364 和 37 的线性组合

(6) $1=6[364-9(37)]-5(37)=6(364)-59(37)$.

用(6)和(1)将 1 写成 364 和 795 的线性组合

(7) $1=6(364)-59[765-2(364)]=124(364)-59(765)$.

因此 $s=124, t=-59$.

于是 $s=124$ 是$(**)$的惟一解，在这个解上乘 71，并且模 765 化简，得

$$124(71)=8804\equiv 389 \pmod{765}.$$

这就是$(*)$的惟一解.

最后，在解 $x_1=389$ 上连续两次加上新的模 $m=765$，分别得到下面的两个解

$$x_2=389+765=1154,\quad x_3=1154+765=1919.$$

换句话说，$x_1=389, x_2=1154, x_3=1919$ 组成了方程 $1092x\equiv 213 \pmod{2295}$ 的一个完整的解集.

11.62 解同余方程 $455x\equiv 204 \pmod{469}$.

解 ☞ 首先用带余除法求 $d=\gcd(455,469)=7$，用 $d=7$ 除 204 余数为 1，也就是说 7 不能整除 204，这样方程无解.

11.63 一个男孩卖水果，苹果一只 12 分，梨一只 7 分，假设他卖得 3.21 元. 问：他卖了多少苹果和多少梨？

解 ☞ 设他卖了 x 只苹果和 y 只梨. 由题意得不定方程

$$12x+7y=321. \qquad (*)$$

(因为 x 和 y 仅限于非负整数，所以此方程为不定方程)方程$(*)$等价于同余方程

$$12x\equiv 321 \pmod 7,$$

将此方程模 7 化简得等价方程

$$5x\equiv 6 \pmod 7.$$

检验 $0,1,\cdots,6$ 得方程惟一解

$$x=4.$$

将模 $m=7$ 的倍数加到 4 上得到 x 的可能值，将每一个 x 代入方程得到相应的 y 的值，即

$$x=4, y=39;\quad x=11, y=27;\quad x=18, y=15.$$

因为 $12(25)=400>321$，故 $x\geqslant 25$ 时，$y<0$. 所以一共有 3 组可能的解

4 个苹果，39 个梨；　11 个苹果，27 个梨；　18 个苹果，15 个梨；

换句话说，

$$x=4+7t,\quad y=39-12t$$

是(*)的通解,仅当$t=0,1,2$时,x、y的值才非负.

11.64 求一个最小正整数x使得它除3余2,除7余4,除10时余6.

解 ☞ 我们来求下面三个方程的最小的正的公共解

$$(a)\ x\equiv 2(\bmod 3);\quad (b)\ x\equiv 4(\bmod 7);\quad (c)\ x\equiv 6(\bmod 10).$$

注意到模3,7和10两两互素.由中国剩余定理(CRT)11.28知,方程对于模$m=3(7)(10)=210$有惟一解,用两种方法解这个问题.

方法1 首先用中国剩余定理来解前两个方程

$$(a)\ x\equiv 2(\bmod 3),\quad (b)\ x\equiv 4(\bmod 7).$$

我们知道方程组模$M=3\cdot 7=21$有惟一解,在第二个方程(b)的解$x=4$上加上模$m=7$的倍数,我们得到下面几个小于21的解

$$4,\quad 11,\quad 18.$$

将这些解代入方程(a)检验,得11是两个方程的惟一解.

用同样的过程来解下面两个方程

$$(c)\ x\equiv 6(\bmod 10),\quad (d)\ x\equiv 11(\bmod 21).$$

由剩余定理得方程组模$M=21\cdot 10=210$有惟一解,在(d)的解$x=11$上加上模$m=21$的倍数,得到10个小于210的(d)的解

$$11,\ 32,\ 53,\ 74,\ 95,\ 116,\ 137,\ 158,\ 179,\ 210.$$

把这些解代入(c)得,$x=116$是方程(c)的惟一解,因此

$$x=104$$

是满足三方程(a),(b)和(c)的最小正整数解.

方法2 运用公式11.29得

$$M=3\cdot 7\cdot 10=210,\quad M_1=210/3=70,$$
$$M_2=210/7=30,\quad M_3=210/10=21.$$

我们来求下列方程组的解

$$70x\equiv 1(\bmod 3),\quad 30x\equiv 1(\bmod 7),\quad 21x\equiv 1(\bmod 10).$$

将70模3化简,30模7化简,21模10化简得等价方程组

$$x\equiv 1(\bmod 3),\quad 2x\equiv 1(\bmod 7),\quad x\equiv 1(\bmod 10).$$

这三个方程的解分别是,

$$s_1=1,\quad s_2=4,\quad s_3=1.$$

代入公式

$$x_0=M_1s_1r_1+M_2s_2r_2+\cdots+M_ks_kr_k$$

得到原方程组的解

$$x_0=70\cdot 1\cdot 2+30\cdot 4\cdot 4+21\cdot 1\cdot 6=746.$$

用模$M=210$除这个解,得余数

$$x=116.$$

即为原方程在0到210之间的惟一解.

11.65 证明定理11.25:如果a和m互素,那么$ax\equiv 1(\bmod m)$有惟一解;否则无解.

证 ☞ 设x_0是一个解,那么m整除$1-ax_0$.因此存在y_0,使得$my_0=1-ax_0$.因此

$$ax_0+my_0=1 \tag{1}$$

且a和m互素.反之,如果a和m互素,则存在x_0和y_0满足(1),在此情况下x_0是$ax\equiv 1(\bmod m)$的一个解.

现在还需证x_0是方程模m的惟一解.设x_1是另一解,那么

$$ax_0\equiv 1\equiv ax_1(\bmod m).$$

由于a,m互素,修正消去律成立,所以

$$x_0\equiv x_1(\bmod m).$$

定理得证.

11.66 证明定理11.26:设a和m互素,那么$ax\equiv b(\bmod m)$有惟一解,进而,如果s是$ax\equiv 1(\bmod m)$的惟一解,那么$x=bs$是$ax\equiv b(\bmod m)$的惟一解.

证 ☞　由定理 11.25(在问题 11.65 中证明),$ax\equiv 1(\bmod m)$的惟一解 s 存在.因此,$as\equiv 1(\bmod m)$,所以

$$a(bs)=(as)b\equiv 1\cdot b=b(\bmod m).$$

也就是说,$x=bs$ 是 $ax\equiv b(\bmod m)$的一个解.假设 x_0 和 x_1 是两个这样的解,那么

$$ax_0\equiv b\equiv ax_1(\bmod m).$$

由于 a 和 m 互素利用修正消去律得 $x_0\equiv x_1(\bmod m)$,也就是说,$ax\equiv b(\bmod m)$有模 m 惟一解.

11.67　证明定理 11.27:考虑方程

$$ax\equiv b(\bmod m). \qquad (*)$$

$d=\gcd(a,m)$,(i) 如果 d 不能整除 b,那么(*)无解.(ii) 如果 d 整除 b,那么(*)有 d 个解,且它们模 m 都与下面这一方程的解同余

$$Ax\equiv B(\bmod M). \qquad (**)$$

$A=a/d$,　$B=b/d$ 且 $M=m/d$.

证 ☞　(i) 设 x_0 是(*)的一个解,那么 $ax_0\equiv b(\bmod m)$,即 m 整除 ax_0-b,这样就存在整数 y_0 使得 $my_0=b-ax_0$ 或 $my_0+ax_0=b$.但 $d=\gcd(a,m)$,所以 d 整除 my_0+ax_0.也就是说 d 整除 b,因此若 d 不整除 b,则方程就无解.

(ii) 设 x_0 是(*)的解,那么如上,

$$my_0+ax_0=b.$$

将方程中每个数都除以 d 得(**),因此 M 整除 Ax_0-B,x_0 是(**)的解.设 x_1 是(**)的解,那么同样存在整数 y_1,使得,

$$My_1+Ax_1=B.$$

在上式上乘以 d 得,

$$dMy_1+dAx_1=dB \quad 即 \quad my_1+ax_1=b.$$

因此 m 整除 ax_1-b,即 x_1 是(*)的解,故(**)有同样的整数解.设 x_0 是(**)的最小的惟一的整数解,既然 $m=dM$,

$$x_0,x_0-M,x_0+2M,x_0+3M,\cdots,x_0+(d-1)M$$

就是方程(**)和(*)的介于 0 与 m 之间的解.因此(*)模 m 有 d 个解,并且模 M 与 x_0 同余.

11.68　证明中国剩余定理(定理 11.28):设方程组

$$x\equiv r_1(\bmod m_1),\quad x\equiv r_2(\bmod m_2),\cdots,x\equiv r_k(\bmod m_k). \qquad (1)$$

其中 m_i 两两互素,那么该方程组模 $M=m_1m_2\cdots\cdots m_k$ 有惟一解.

证 ☞　考察整数

$$x_0=M_1s_1r_1+M_2s_2r_2+\cdots+M_ks_kr_k.$$

其中 $M_i=M/m_i$,s_i 是方程 $M_ix\equiv 1(\bmod m_i)$的惟一解.对于给定的 j,$i\neq j$,有 $m_j|M_i$,因此

$$M_is_ir_i\equiv 0(\bmod m_j).$$

另一方面,$M_js_j\equiv 1(\bmod m_j)$,于是

$$M_js_jr_j\equiv r_j(\bmod m_j).$$

所以,

$$x_0\equiv 0+\cdots+0+r_j+0+\cdots+0\equiv r_j(\bmod m_j).$$

换句话说,x_0 是(1)中每一个方程的解.

现在我们还需证明 x_0 是方程组(1)的模 M 惟一解,设 x_1 是(1)中所有方程的另一解,那么

$$x_0\equiv x_1(\bmod m_1),x_0\equiv x_1(\bmod m_2),\cdots,x_0\equiv x_1(\bmod m_k).$$

因此 $m_i|(x_0-x_1)$,对每一个 i.由于 m_i 两两互素,$M=\text{lcm}(m_1,m_2,\cdots,m_k)$.所以 $M|(x_0-x_1)$,即

$$x_0\equiv x_1(\bmod M).$$

定理得证.

补 充 题

序和不等式，绝对值

11.69 在各对整数间填入恰当的符号：<，>或=.

(a) 2 ____ −6，　(b) −3 ____ −5，　(c) −7 ____ +3，　(d) −8 ____ −1，

(e) 2^3 ____ 11，　(f) 2^3 ____ −9，　(g) −2 ____ −7，　(h) 4 ____ −9.

11.70 计算：(a) $|-6|,|5|,|0|$；(b) $|3-7|,|-3+7|,|-3-7|$.

11.71 计算：(a) $|2-5|+|3+7|,|1-4|-|2-9|$；(b) $|-4|+|2-3|,|-6-2|-|2-6|$.

11.72 求每对整数间的距离 d

(a) 2 和 −5；(b) −6 和 3；(c) 2 和 8；(d) −7 和 −1；(e) 3 和 −3；(f) −7 和 −9.

11.73 分别求满足下列两式的整数 n：(a) $3<2n-4<10$；(b) $1<6-3n<13$.

11.74 证明性质 11.1：(i) 对于任何整数 a，$a\leqslant a$；(ii) 如果 $a\leqslant b$，$b\leqslant a$，那么 $a=b$.

11.75 证明性质 11.2：对于任何整数 a 和 b，一定满足下面关系中的一种：$a<b$，$a=b$，或 $a>b$.

11.76 证明：(a) $2ab\leqslant a^2+b^2$；(b) $ab+ac+bc\leqslant a^2+b^2+c^2$.

11.77 性质 11.4：(i) $|a|\geqslant 0$ 且 $|a|=0$ 当且仅 $a=0$. (ii) $-|a|\leqslant a\leqslant |a|$ (iii) $||a|-|b||\leqslant |a\pm b|$.

11.78 证明：如果 $b\neq 0$ 且 $x=-|a|b$，则 $a-xb\geqslant 0$

数学归纳法，良序原理

11.79 证明前 n 个正偶数的和是 $n(n+1)$，即

$$P(n): 2+4+6+\cdots+2n=n(n+1).$$

11.80 证明前 n 个正整数的立方和等于前 n 个数和的平方，即

$$P(n): 1^3+2^3+3^3+\cdots+n^3=(1+2+\cdots+n)^2.$$

11.81 证明：$1+4+7+\cdots+(3n-2)=n(3n-1)/2$.

11.82 证明：(a) $a^na^m=a^{n+m}$；(b) $(a^n)^m=a^{nm}$；(c) $(ab)^n=a^nb^n$.

11.83 证明：$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$.

11.84 证明：$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\frac{1}{5\cdot 7}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}$.

11.85 证明：$\frac{1^2}{1\cdot 3}+\frac{2^2}{3\cdot 5}+\frac{3^2}{5\cdot 7}+\cdots+\frac{n^2}{(2n-1)(2n+1)}=\frac{n(n+1)}{2(2n+1)}$.

11.86 证明：

(a) $x^{n+1}-y^{n+1}=(x-y)(x^n+x^{n-1}y+x^{n-2}y^2+\cdots+y^n)$.

(b) $a^{n+1}+b^{n+1}=(a+b)(a^n-a^{n-1}b+a^{n-2}b^2-\cdots-ab^{n-1}+b^n)$.

11.87 证明：$|P(A)|=2^n$，这里 $|A|=n$.（$P(A)$ 是含有 n 个元素的有限集 A 的幂集.）

带余除法

11.88 对每一对整数 a 和 b，求整数 q 和 r 使得 $a=bq+r$ 且 $0\leqslant r<|b|$.

(a) $a=395, b=14$.　(b) $a=608, b=-17$.

(c) $a=-278, b=12$.　(d) $a=-417, b=-8$.

11.89 证明下列命题：

(a) 任意整数 a 都可写成 $5k$，$5k+1$，$5k+2$，$5k+3$ 和 $5k+4$ 的形式.

(b) 每 5 个连续的整数必有一个是 5 的倍数.

11.90 证明下列命题：

(a) 任意 3 个连续整数的积都能被 6 整除.

(b) 任意 4 个连续整数的积必被 24 整除.

11.91 证明下列数不是有理数：

(a) $\sqrt{3}$；(b) $\sqrt[3]{2}$.

11.92 证明：$\sqrt{p}$ 不是有理数，其中 p 是任一素数.

整除,最大公因数和素数

11.93 求所有可能的因子:(a) 24;(b) $19683=3^9$;(c) $432=2^4\cdot 3^3$.

11.94 写出 100 到 150 之间的所有素数.

11.95 将下列各数写成素数积:

(a) 2940; (b) 1485; (c) 8712; (d) 319410.

11.96 对于每对整数 a,b,求 $d=\gcd(a,b)$,并将 d 写成 a,b 的线性组合.

(a) $a=48,b=356$, (b) $a=165,b=1287$,

(c) $a=2310,b=168$, (d) $a=195,b=968$.

11.97 求:(a) $\mathrm{lcm}(5,7)$;(b) $\mathrm{lcm}(3,33)$;(c) $\mathrm{lcm}(12,28)$.

11.98 设 $a=5880$ 和 $b=8316$,

(a) 将 a 和 b 写成素数积形式.

(b) 求 $\gcd(a,b)$ 和 $\mathrm{lcm}(a,b)$.

(c) 证明 $\mathrm{lcm}(a,b)=(|ab|)/\gcd(a,b)$.

11.99 证明:(a) 如果 $a|b$,那么 $a|-b,-a|b,-a|-b$. (b) 如果 $ac|bc$,那么 $a|b$.

11.100 证明:

(a) 如果 $n(>1)$是合数,那么 n 有正因子 d 使得 $d\leqslant\sqrt{n}$.

(b) 如果 $n(>1)$不能被任一素数 $p\leqslant\sqrt{n}$整除,那么 n 是素数.

11.101 证明:(a) 如果 $am+bn=1$,那么 $\gcd(a,b)=1$. (b) 如果 $a=bq+r$,那么$\gcd(a,b)=\gcd(b,r)$.

11.102 证明:(a) $\gcd(a,a+k)$整除 k. (b) $\gcd(a,a-2)=1$ 或 2.

11.103 证明:

(a) 如果 $a>2,k>1$,那么 a^k-1 是合数.

(b) 如果 $n>0,2^n-1$ 是素数,那么 n 是素数.

11.104 设 n 是正整数,证明:

(a) 3 整除 n 当且仅当 n 中各位数字之和能被 3 整除.

(b) 9 整除 n 当且仅当 n 中各位数字之和能被 9 整除.

(c) 8 整除 n 当且仅当 n 的后 3 位数能被 8 整除.

11.105 把 gcd 和 lcm 的定义扩展到任意有限整数集上,即对于整数 $a_1,a_2\cdots a_k$,定义:

(a) $\gcd(a_1,a_2,\cdots,a_k)$; (b) $\mathrm{lcm}(a_1,a_2,\cdots,a_k)$.

11.106 证明:如果 $a_1|n,a_2|n,\cdots,a_k|n$,那么 $m|n$. 其中 $m=\mathrm{lcm}(a_1,\cdots,a_k)$.

11.107 证明:素数间的距离可以任意大,也就是说对于任何正整数 k,存在 k 个连续的合数(非素数).

同余

11.108 下列各式哪些是正确的?

(a) $224\equiv762(\bmod 8)$, (b) $582\equiv263(\bmod 11)$,

(c) $156\equiv-369(\bmod 7)$, (d) $-238\equiv483(\bmod 13)$.

11.109 求与下列各数模 9 同余的最小非负整数:

(a) 457;(b) 1578;(c) −366;(d) −3288.

(所求整数应在集合$\{0,1,2,\cdots,7,8\}$中)

11.110 求与下列各数模 9 同余的绝对值最小的整数:

(a) 511;(b) 1329;(c) −625;(d) −2717.

(所求整数应在集合$\{-4,-3,-2,-1,0,1,2,3,4\}$中)

11.111 求 1 到 100 之间,模 $m=11$ 余 4 的所有整数.

11.112 求−50 与 50 之间,模 $m=9$ 余 12 的所有整数.

剩余类和欧拉函数$\varnothing$

11.113 对于每一个模 m 写出它的两个完全剩余系,一个由最小的非负整数组成,另一个由绝对值最小的整数组成:(a) $m=11$;(b) $m=14$.

11.114　写出模 m 的简化剩余系并求$\varnothing(m)$：(a) $m=4$；(b) $m=11$；(c) $m=14$；(d) $m=15$.

11.115　写出模 $m=8$ 的一个完全剩余系，由下列数组成.

(a) 5 的倍数；(b) 3 的幂.

11.116　证明：$\{1^2,2^2,\cdots,m^2\}$不是模 $m(>2)$的一个完全剩余系.

11.117　求：(a) $\varnothing(10)$；(b) $\varnothing(12)$；(c) $\varnothing(15)$.

11.118　求：(a) $\varnothing(3^7)$；(b) $\varnothing(5^6)$；(c) $\varnothing(2^4\cdot 7^6\cdot 13^3)$.

11.119　求小于 3200 且与 800 互素的所有正整数的个数 s.

模 m 的运算，$\mathbf{Z}_m$

11.120　写出加法表和乘法表：(a) $\mathbf{Z}_2$；(b) $\mathbf{Z}_8$.

11.121　在 $\mathbf{Z}_{13}$中求：(a) $-2,-3,-5,-9,-10,-11$；(b) $2/9,4/9,5/9,7/9,8/9$.

11.122　在 $\mathbf{Z}_{17}$中求：(a) $-3,-5,-6,-8,-13,-15,-16$；(b) $3/8,5/8,7/8,13/8,15/8$.

11.123　在 $\mathbf{Z}_m$ 中求 a^{-1}：(a) $a=15,m=127$；(b) $a=61,m=124$；(c) $a=12,m=111$.

11.124　在 $\mathbf{Z}_5$ 上求积 $f(x)g(x)$：$f(x)=4x^3-2x^2+3x-1,g(x)=3x^2-x-4$.

同余方程

11.125　解下列同余方程：

(a) $f(x)=2x^3-x^2+3x+1\equiv 0(\mathrm{mod}\ 5)$.

(b) $g(x)=3x^4-2x^3+5x^2+x+2\equiv 0(\mathrm{mod}\ 7)$.

(c) $h(x)=45x^3-37x^2+26x+312\equiv 0(\mathrm{mod}\ 6)$.

11.126　解下列线性同余方程：

(a) $7x\equiv 3(\mathrm{mod}\ 9)$；(b) $4x\equiv 6(\mathrm{mod}\ 14)$；(c) $6x\equiv 4(\mathrm{mod}\ 9)$.

11.127　解下列线性同余方程：

(a) $5x\equiv 3(\mathrm{mod}\ 8)$；(b) $6x\equiv 9(\mathrm{mod}\ 16)$；(c) $9x\equiv 12(\mathrm{mod}\ 21)$.

11.128　解下列线性同余方程：

(a) $37x\equiv 1(\mathrm{mod}\ 249)$；　(b) $195x\equiv 23(\mathrm{mod}\ 968)$.

11.129　解下列线性同余方程：

(a) $132x\equiv 169(\mathrm{mod}\ 735)$；(b) $48\equiv 284(\mathrm{mod}\ 356)$.

11.130　一个木偶剧院只有 60 个座位，门票价格是成人 2.25 元，小孩 1.00 元，假设总收入是 117.25 元，问看演出的成人和小孩各有多少人？

11.131　求下列每组同余方程组的最小正整数解：

(a) $x\equiv 2(\mathrm{mod}\ 3),x\equiv 3(\mathrm{mod}\ 5),x\equiv 4(\mathrm{mod}\ 11)$.

(b) $x\equiv 3(\mathrm{mod}\ 5),x\equiv 4(\mathrm{mod}\ 7),x\equiv 6(\mathrm{mod}\ 9)$.

11.132　求下面这个同余方程组的最小正整数解：

$x\equiv 5(\mathrm{mod}\ 45)$；$x\equiv 6(\mathrm{mod}\ 49)$；$x\equiv 7(\mathrm{mod}\ 52)$.

补充题答案

11.69　(a) $2>-6$；　(b) $-3>-5$；　(c) $-7<3$；　(d) $-8<-1$.

(e) $2^3<11$；　(f) $2^3>-9$；　(g) $-2>-7$；　(h) $4>-9$.

11.70　(a) 6,5,0；(b) 4,4,10.

11.71　(a) $3+10=13,3-7=-4$；(b) $4-1=5,8-4=4$.

11.72　(a) 7；(b) 9；(c) 6；(d) 6；(e) 6；(f) 3.

11.73　(a) 4,5,6；(b) $-2,-1,0,1$.

11.88　(a) $q=28,r=3$；(b) $q=-15,r=13$；(c) $q=-24,r=10$；(d) $q=53,r=7$.

11.90　(a) 一个被 2 整除，一个被 3 整除.

(b) 一个被 4 整除，一个被 2 整除，另一个被 3 整除.

11.93　(a) 1,2,3,4,6,12,24；(b) $3^n(n=1,2,3,\cdots,9)$；(c) $2^r3^s(r=0,1,2,3,4,s=0,1,2,3)$.

11.94　101,103,107,109,113,127,131,137,139,149.

11.95 (a) $2940=2^2\cdot 3\cdot 5\cdot 7^2$;(b) $1485=3^3\cdot 5\cdot 11$;(c) $8712=2^3\cdot 3^2\cdot 11^2$;

(d) $319410=2\cdot 3^3\cdot 5\cdot 7\cdot 13^2$.

11.96 (a) $d=4=5(356)-37(48)$;　(b) $d=33=8(165)-1(1287)$;

(c) $d=42=14(168)-1(2310)$; (d) $d=1=139(195)-28(968)$.

11.97 (a) 35;(b) 33;(c) 84.

11.98 (a) $a=2^4\cdot 3\cdot 5\cdot 7^2, b=2^2\cdot 3^3\cdot 7\cdot 11$.

(b) $\gcd(a,b)=2^2\cdot 3\cdot 7, \mathrm{lcm}(a,b)=2^4\cdot 3^3\cdot 5\cdot 7^2\cdot 11=1164240$.

11.103 (a) 提示:$a^k-1=(a-1)(1+a+a^2+\cdots+a^{k-1})$.

(b) 提示:如果 $n=ab$,那么 $2^n-1=(2^a)^b-1$.

11.107 $(k+1)!+2,(k+1)!+3,(k+1)!+4,\cdots,(k+1)!+(k+1)$分别被 $2,3,4,\cdots,k+1$ 整除.

11.108 (a) 错误;(b) 正确;(c) 正确;(d) 错误.

11.109 (a) 7;(b) 2;(c) 3;(d) 6.

11.110 (a) -2;(b) -3;(c) -2;(d) 1.

11.111 4,15,26,37,48,59,70,81,92.

11.112 $-42,-33,-24,-15,-6,3,12,21,30,39,48$.

11.113 (a) $\{0,1,\cdots,10\}$和$\{-5,-4,\cdots,-1,0,1,\cdots,4,5\}$

(b) $\{0,1,\cdots,13\}$和$\{-6,-5,\cdots,-1,0,1,\cdots 6,7\}$

11.114 (a) $\{1,3\}$;(b) $\{1,2,\cdots,10\}$;(c) $\{1,3,5,9,11,13\}$;(d) $\{1,2,4,7,8,11,13,14\}$.

11.115 (a) $\{5,10,15,20,25,30,35,40\}$;(b) $\{3,9,27,81,243,729,2187,6561\}$.

11.116 $m-1\equiv -1(\bmod m)$,因此$(m-1)^2\equiv(-1)^2=1^2(\bmod m)$.

11.117 (a) $\varnothing(10)=4$;(b) $\varnothing(12)=4$;(c) $\varnothing(15)=8$.

11.118 (a) $\varnothing(3^7)=2\cdot 3^6$;(b) $\varnothing(5^6)=4\cdot 5^5$;(c) $\varnothing(2^4\cdot 7^6\cdot 13^3)=(2^3)(6\cdot 7^5)(12\cdot 13^2)$.

11.119 $\varnothing(8000)=\varnothing(2^6\cdot 5^3)=2^5\cdot 4\cdot 5^2=320$,因此 $s=4(320)=1280$.

11.121 (a) $-2=11$,　$-3=10$,　$-5=8,-9=4,-10=3,-11=2$.

(b) (提示:先求出 9 模 13 的乘法表)

$2/9=6$,　$4/9=12$,　$5/9=2$,　$7/9=8$,　$8/9=11$.

11.122 (a) $-3=14$,　$-5=12$,　$-6=11$,　$-8=9$,　$-13=4$,　$-15=2$.

(b) $3/8=11$,　$5/8=7$,　$7/8=3$,　$13/8=8$,　$15/8=4$.

11.123 (a) $a^{-1}=17$;　(b) $a^{-1}=61$;　(c) a^{-1}不存在.

11.124 $f(x)g(x)=2x^5+2x^2-x+4$.

11.125 (a) 1,3,4;　(b) $2,-2$;　(c) $0,2,3,-1$.

11.126 (a) 3;　(b) 5,12　(c)无解.

11.127 (a) 7;　(b) 无解　(c) 6,13,20.

11.128 (a) 175;　(b) 293.

11.129 (a) 无解;　(b) 43,132,221,310.

11.130 12 个成人和 47 个小孩或 3 个成人和 51 个小孩.

11.131 (a) 158;　　(b) 123.

11.132 31415.

第十二章 代数系统

12.1 引 言

本章研究数学中的一些主要的代数系统:半群,群,环和域.还要给出同态和商结构的定义.我们首先给出运算的定义,讨论各种类型的运算.

12.2 运 算

读者很熟悉数的加法与乘法运算,集合的并与交以及函数的复合.这些运算定义如下

$$a+b=c,\quad a\cdot b=c,\quad A\cup B=C,\quad A\cap B=C,\quad g\bigcirc f=h.$$

在每一种情况下,一个元素(c,C 或 h)都对应着原来的一对元素.换句话说,在每一个函数中都将已知的一对元素对应着一个惟一的元素.我们给出明确的定义.

定义 设 S 是一个非空集合,集合 S 上的一个运算是 $S\times S$ 到 S 的一个函数 $*$,通常记

$$a*b \quad 或 \quad ab,$$

而不记为 $*(a,b)$.集合 S 和 S 上的一个运算 $*$ 记为 $(S,*)$ 或当运算明确时简记为 S.

注 一个从 $S\times S$ 到 S 上的运算 $*$ 有时称为二元运算.一元运算是从 S 到 S 的函数,例如,整数 n 的绝对值 $|n|$ 就是 $\mathbf{Z}$ 上的一个一元运算,集合 A 的补 A^C 是集合 X 的幂集 $P(X)$ 上的一个一元运算.三元运算是从 $S\times S\times S$ 到 S 的一个函数.更一般地,n 元运算是从 $S\times S\times\cdots\times S$($n$ 个)到 S 的一个函数.除特别指明,运算都是指二元运算,并且假设所论基础集合 S 非空。

设 S 是有限集.则 S 上的运算 $*$ 可以通过它的运算(乘法)表给出,若行标为 a,列标为 b,则对应的数为 $a*b$.

设 S 是具有运算 $*$ 的集合,且令 A 是 S 的子集.如果对于集合 A 中的任意元素 a 和 b 有 $a*b$ 属于 A,则称 A 关于运算 $*$ 封闭.

例 12.1 考虑正整数集 $\mathbf{N}$.

(a) 加法(+)和乘法(×)是 $\mathbf{N}$ 上的运算,但是减法(−)和除法(/)不是 $\mathbf{N}$ 上的运算.因为正整数的差或商不一定是正整数,比如 $2-9$ 和 $7/3$ 都不是正整数。

(b) 设 A,B 分别表示正偶数和正奇数的集合、则由于任何偶数的和与积仍为偶数,故 A 关于加法与乘法封闭;但是 B 关于乘法封闭而关于加法不封闭,如 $3+5=8$ 是偶数.

例 12.2 (a) 设 $S=\{0,1,-1\}$.那么由于 $1+1$ 不是 S 中的元素,加法(+)不是 S 上的运算,但乘法(×)是 S 上的运算.

(b) 设 S 表示所有整数的 2×2 矩阵的集合

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

那么矩阵的加法和乘法是 S 上的运算。设 A 和 B 分别为 S 的子集,形式如下

$$\begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \quad 和 \quad \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}.$$

则 A 关于矩阵加法封闭,乘法不封闭,比如

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}=\begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix}.$$

而 B 关于矩阵加法和乘法都封闭.

例 12.3 设 $S=\{a,b,c,d\}$,图 12-1 的表中定义了 S 上的运算 $*$ 和 $\cdot$,注意 $*$ 可由公式

$$x * y = x$$

定义，其中 x,y 是 S 中的任意元素.

*	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

(a)

·	a	b	c	d
a	a	b	c	d
b	b	a	a	b
c	c	b	a	a
d	d	a	a	a

(b)

图 12-1

运算的性质

下面列出运算的一些重要性质.

(1) 结合律和交换律

集合 S 上的运算 $*$ 称为*可结合的*或*满足结合律*，如果对于 S 中任意元素 a,b,c，有

$$(a*b)*c = a*(b*c).$$

一般地，如果一个运算不是可结合的，则可有许多方法构成一个积，例如下面给出了 5 种形成积 $abcd$ 的方法：

$$((ab)c)d,\quad (ab)(cd),\quad (a(bc))d,\quad a((bc)d),\quad a(b(cd)).$$

如果一个运算是可结合的，则有下面的定理(在问题 12.7 中证明).

定理 12.1 设 $*$ 是集合 S 上的一个可结合的运算，那么任何积 $a_1 * a_2 * \cdots * a_n$ 无须加括号，也就是说所有可能的积都相等.

集合 S 上的运算 $*$ 称为*可交换的*或*满足交换律*，如果对 S 中任意元素 a,b 有

$$a*b = b*a.$$

例 12.4 (a) 考虑整数集 **Z**，整数的加法和乘法是可结合的和可交换的，而减法是不可结合的，比如，

$$(8-4)-3 = 1 \quad 但 \quad 8-(4-3) = 7.$$

另外减法也是不可交换的，比如 $3-7 \neq 7-3$.

(b) 考虑 n 阶方阵集合 M 上的矩阵乘法运算，可以证明(见 5.5 节)矩阵乘法是可结合的. 但矩阵乘法是不可交换的，例如

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}5 & 6\\0 & -2\end{bmatrix} = \begin{bmatrix}5 & 2\\15 & 10\end{bmatrix} \quad 但 \quad \begin{bmatrix}5 & 6\\0 & -2\end{bmatrix}\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix} = \begin{bmatrix}23 & 34\\-6 & -8\end{bmatrix}.$$

(c) 考虑正整数集 **N** 上的指数运算 $a*b=a^b$，这个运算不是可结合的，例如

$$(2*2)*3=(2^2)^3=4^3=64 \quad 但 \quad 2*(2*3)=2^{2^3}=2^8=256.$$

另外，$*$ 也不是可交换的，例如，

$$2*3 = 2^3 = 8 \quad 但 \quad 3*2 = 3^2 = 9.$$

(d) 考虑由图 12-1(b)定义的集合 $S=\{a,b,c,d\}$ 上的运算，该运算不是可结合的. 例如，

$$(b\cdot c)\cdot c = a\cdot c = c \quad 但 \quad b\cdot(c\cdot c) = b\cdot a = b.$$

另外，此运算也不是可交换的，例如 $b\cdot c=a$ 但 $c\cdot b=b$.

(2) 单位元和逆元

考虑集合 S 上的运算 $*$，S 中的元素 e 称为 $*$ 的*单位元*，如果对于 S 中的任意元素 a，有

$$a*e = e*a = a.$$

更一般地，对于 S 中的任意元素 a，如果 $e*a=a$，则 e 称为*左单位元*；如果 $a*e=a$ 则 e 称为*右单位元*. 我们有下面的定理.

定理 12.2 设 e 是左单位元，f 是右单位元，那么 $e=f$.

证明是很简单的. 由于 e 是左单位元，$ef=f$；但又因 f 是右单位元，故 $ef=e$，于是 $e=f$. 本定理特别指出单位元是惟一的，即若有多于一个左单位元，则没有右单位元；反之亦然.

设集合 S 上的运算 $*$ 有单位元 e，那么 S 中元素 a 的*逆元*是元素 b，满足

$$a*b=b*a=e.$$

如果运算是可结合的，那么 a 的逆元，若存在则惟一（问题 12.3）. 显然，如果 b 是 a 的逆元，那么 a 是 b 的逆元，因此逆元是一个对称关系，我们可以说元素 a 和 b 互逆.

注 如果 S 上的运算记成 $a*b$，$a\times b$，$a\cdot b$ 或 ab，则称 S 为*乘法式结构*，S 中元素 a 的逆记为 a^{-1}. 有时，当 S 可交换时，运算记为 $+$，称 S 为*加法式结构*. 在这种情况下单位元通常记为 0，称之为*零元素*. a 的逆元记为 $-a$，且称为 a 的*负元素*.

例 12.5 (a) 考虑有理数集 **Q**. 在加法下，0 是单位元，且 -3 与 3 互逆，因为

$$(-3)+3=3+(-3)=0$$

另外，在乘法下，1 是单位元，-3 和 $-\frac{1}{3}$ 互逆，因为

$$(-3)\cdot\left(-\frac{1}{3}\right)=\left(-\frac{1}{3}\right)\cdot(-3)=1.$$

注意，0 没有乘法式结构逆元.

(b) 考虑具有如图 12-1(b)定义运算的集合 $S=\{a,b,c,d\}$，可见元素 a 是单位元，而且由 $dd=a$，知 d 是它本身的逆元. 进一步，$dc=cd=a$，所以 c 和 d 也互逆，因此 d 的逆元不惟一.（这就意味着此运算不是可结合.）

(3) *消去律*

称集合 S 上的运算 $*$ 满足*左消去律*，如果

$$a*b=a*c \quad 蕴含 \quad b=c.$$

满足右消去律，如果

$$b*a=c*a \quad 蕴含 \quad b=c.$$

整数集 **Z** 上的加法，减法和乘法既满足左消去律也满足右消去律。但矩阵的乘法不满足消去律，例如，设

$$A=\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix},\ B=\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix},\ C=\begin{bmatrix}0 & -3\\1 & 5\end{bmatrix},\ D=\begin{bmatrix}1 & 2\\0 & 0\end{bmatrix}.$$

那么 $AB=AC=D$，但 $B\neq C$.

12.3 半 群

设 S 是定义了一个运算的非空集合，若该运算是可结合的则称 S 为*半群*；若该运算还有一个单位元，则称 S 为*幺半群*.

例 12.6 (a) 考虑正整数集 **N**，那么由于 **N** 上的加法和乘法是可结合的，故(**N**, +)和(**N**, ×)是半群. 特别地，(**N**, ×)是幺半群，因为有单位元 1. 而(**N**, +)不是幺半群，因 **N** 中的加法没有零元.

(b) 设 S 是一个有限集，$F(S)$ 为所有函数 $f:S\to S$，且运算为函数的复合. 因为函数的复合可结合，$F(S)$ 是半群. 事实上，$F(S)$ 是一个幺半群，因为恒等函数是 $F(S)$ 的一个单位元.

(c) 设 $S=\{a,b,c,d\}$. 图 12-1 的乘法表定义了 S 上的运算 $*$ 和 $\cdot$. 注意到 $*$ 可以由公式 $x*y=x$ 对于 S 中的任意 x 和 y 定义，因此

$$(x*y)*z=x*z=x,\ x*(y*z)=x*y=x.$$

因此，$*$ 是可结合的，所以 $(S,*)$ 是一个半群. 另一方面 $\cdot$ 是不是可结合的，例如

$$(b \cdot c) \cdot c = a \cdot c = c \quad 但 \quad b \cdot (c \cdot c) = b \cdot a = b.$$

因此(S·)不是一个半群.

自由半群,自由幺半群

设A是一非空集合,A上的一个字符串(简称串)w是A中元素的一个有限序列.例如

$$u = ababbbb = abab^4, \quad v = baccaaaa = bac^2a^4$$

是$A=\{a,b,c\}$上的串.(我们把aa写成a^2,aaa写成a^3,等等).一个串w的长度记为$L(w)$,即w中元素的个数,于是$l(u)=7$,$l(v)=8$.

集合A上串u和v的连接,记为$u*v$或uv,即将v接在u后面所得到的串,例如,

$$uv = (abab^4)(bac^2a^4) = abab^5ac^2a^4.$$

现设$F=F(A)$表示A上所有字符串在连接运算下的集合.显然对于任意串u,v,w,串$(uv)w$和$u(vw)$是一样的;它们都是由u,v,w一个接一个地写成的,因此F是一个半群,称为A上的自由半群,A的元素,称为F的生成元.

空序列记为λ,也看做A上的一个串.但我们不能认为λ属于自由半群$F=F(A)$.A上所有的串包括λ记为A^*.于是A^*是连接下的一个幺半群,称为A上的自由幺半群.

子半群

设A是半群S的一个非空子集,如果A本身对于S上的运算是一个半群则称A为S的一个子半群.因为A中的元素也是S的元素,A中元素自然满足结合律。因此A是一子半群当且仅当其在S的运算下封闭.

例 12.7 (a) 设A和B分别表示正奇数集和正偶数集.因为A和B关于乘法封闭,所以$(A,\times)$和$(B,\times)$是$(\mathbf{N},\times)$的子半群.另外,由于A关于加法封闭,所以$(A,+)$是$(\mathbf{N},+)$的子半群,但$(B,+)$不是$(\mathbf{N},+)$的子半群,因为B对加法不封闭.

(b) 考虑集合$A=\{a,b\}$上的自由半群F.设H是所有偶串构成的集合,也就是说长度为偶数的串,两个这样的串的连接仍然是偶串.这样H就是F的一个子半群.

同余关系和商结构

设S是一个半群,$\sim$是S上的一个等价关系.回顾等价关系可以把集合S分成等价类,且用$[a]$表示含有集合S中元素a的等价类,等价类的集合记为$S/\sim$.

假设S上的等价关系有下面的性质

如果$a\sim a'$,$b\sim b'$,那么$ab\sim a'b'$.

那么$\sim$称为S上的同余关系,而且可以定义等价类上的一个运算

$$[a]*[b]=[a*b] \quad 或 \quad [a][b]=[ab].$$

并且这个$S/\sim$上的运算是可结合的,因此$S/\sim$是一个半群.此结果的正式叙述如下:

定理 12.3 设$\sim$是半群S上的一个同余关系,那么$\sim$的等价类$S/\sim$关于运算

$$[a][b]=[ab]$$

构成一个半群.这个半群$S/\sim$称为由$\sim$生成的商群.

例 12.8 (a) 设F是一集合A上的自由半群,若u与u'长度相同则定义$u\sim u'$.于是$\sim$是F上的一个等价关系.而且假设$u\sim u'$、$v\sim v'$即.

$$l(u) = l(u') = m, \ l(u) = l(u') = n.$$

那么$l(uv)=l(u'v')=m+n$,所以$uv\sim u'v'$,这样$\sim$是F上的一个同余关系

(b) 考虑整数集$\mathbf{Z}$和一个正整数$m>1$,回顾(11.8节),a模m余b,记作

$$a \equiv b(\mathrm{mod}\ m).$$

如果m整除差$a-b$.定理11.20指出这个关系是$\mathbf{Z}$上的一个等价关系进而定理11.21指出若$a\equiv c(\mathrm{mod}\ m)$,$b\equiv d(\mathrm{mod}\ m)$,则

$$a+b \equiv c+d \pmod{m},\ ab \equiv cd \pmod{m}.$$

换句话说，这个关系是 $\mathbf{Z}$ 上同余关系.

半群的同态

考虑两个半群 $(S,*)$ 和 $(S',*')$. 函数 $f:S \to S'$ 称为半群同态或简称为同态，如果

$$f(a*b)=f(a)*'f(b) \quad 或 \quad f(ab)=f(a)f(b).$$

假设 f 是 1—1 的，映上的. 则 f 称为 S 与 S' 之间的一个同构，S 和 S' 称为同构半群，记作 $S \approx S'$.

例 12.9 (a) 设 F 是 A 上的自由半群，令 $\mathbf{Z}$ 表示具有加法的整数集. 假设

$$f:F \to \mathbf{Z} \text{ 定义为 } f(w)=l(w),$$

那么，由于 $l(uv)=l(u)+l(v)$，所以 f 是一同态，也就是说，对于任何串 u,v，

$$f(uv)=l(uv)=l(u)+l(v)=f(u)+f(v).$$

注意 F 中的运算写成乘法，而 $\mathbf{Z}$ 中的运算则为加法.

(b) 图 12-2(a) 给出了 $\mathbf{Z}_4$ 的加法表，而图 12-2(b) 给出了 $\mathbf{Z}_{10}$ 中 $S=\{1,3,7,9\}$ 的乘法表.（注意 S 是模 10 的简化剩余系）设 $f:\mathbf{Z}_4 - S$ 定义为

$$f(0)=1,\ f(1)=3,\ f(2)=9,\ f(3)=7.$$

可以证明 f 是一个同态，又因为 f 是 1-1 的，映上的，故 f 又是同构的. 于是 $\mathbf{Z}_4$ 和 S 是同构半群.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(a)

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(b)

图 12-2

(c) 设 M 是 2×2 整数矩阵的集合，任意矩阵 $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 的行列式定义为 $\det(A)=|A|=ad-bc$. 线性代数中已证明行列式是一个可乘函数，也就是说，对于任何方阵 A 和 B，

$$\det(AB)=\det(A)\cdot\det(B).$$

因此行列式函数是矩阵的乘法半群 $(M,\times)$ 的一个同态，另外行列式函数不是可加的，即对于某些矩阵，

$$\det(A+B)\neq\det(A)+\det(B)$$

所以行列式函数不是 $(M,+)$ 上的一个半群同态.

(d) 设 $\sim$ 是半群 S 上的一同余关系，设 $\phi:S \to S/\sim$ 是从 S 到商半群 $S/\sim$ 的一个自然映射，定义为

$$\phi(a)=[a].$$

即 S 中的每一个元素 a 都对应着它的等价类 $[a]$. 那么 ϕ 是一个同态，因为

$$\phi(ab)=[ab]=[a][b]=\phi(a)\phi(b).$$

半群同态基本定理

回顾一个函数 $f:S \to S'$ 的像记为 $f(S)$ 或 $\mathrm{Im}f$，表示 S 中元素在 f 下的像构成的集合，即

$$\mathrm{Im}f=\{b\in S':\text{存在 } a\in S \text{ 使 } f(a)=b\}.$$

下面是半群理论的一个基本定理（在问题 12.8 中证明）

定理 12.4 设 $f:S \to S'$ 是一个半群同态，如果 $f(a)=f(b)$，令 $a\sim b$，则

(i) $\sim$是 S 上的同余关系.

(ii) $S/\sim$同构于 $f(S)$.

例 12.10　(a) 设 F 是 $A=\{a,b\}$ 上的自由半群,函数 $f:F\to\mathbf{Z}$ 定义为

$$f(u)=l(u),$$

是一同态,注意 $f(F)=\mathbf{N}$,因此 $F/\sim$同构于 $\mathbf{N}$

(b) 设 M 是 2×2 整数矩阵的集合,考察行列式函数 $\det:M\to\mathbf{Z}$. 对于任何整数 a,有

$$\det\begin{bmatrix}a & 0\\ 0 & 1\end{bmatrix}=a.$$

因此行列式的像是 $\mathbf{Z}$,由定理 12.4 $M/\sim$同构于 $\mathbf{Z}$.

半群的积

设$(S_1,*_1)$和$(S_2,*_2)$是两个半群,我们构造一个新半群 $S=S_1\otimes S_2$,称为 S_1 和 S_2 的*直积*,如下

(1) S 中的元素来自 $S_1\times S_2$,即 S 中的元素是有序偶(a,b),$a\in S_1$,$b\in S_2$.

(2) S 中运算 $*$ 定义为分量两两相乘,即

$(a,b)*(a',b')=(a*_1a',b*_2b')$ 或简记为 $(a,b)(a',b')=(aa',bb')$.

容易证明上面的运算是可结合的.

12.4　群

设 G 是定义了二元运算(用并置表示)的非空集合,则 G 称为*群*,如果满足下列公理:

[$\mathbf{G}_1$] *结合律*　对任何元素 $a,b,c\in G$,有$(ab)c=a(bc)$.

[$\mathbf{G}_2$] *单位元*　存在元素 $e\in G$,使得对于 G 中每一个元素 a. 有 $ae=ea=a$.

[$\mathbf{G}_3$] *逆元*　对每一个元素 $a\in G$,存在一个元素 $a^{-1}\in G$(a 的逆元)使得

$$aa^{-1}=a^{-1}a=e.$$

若群 G 满足交换律即对于任意的 $a,b\in G$ 有 ,$ab=ba$,则称 G 为*阿贝尔群*(或*交换群*).

当二元运算如上并置定义时,称 G 为*乘法群*. 当 G 是阿贝尔群时,运算记为$+$,称 G 为*加法群*. 此时单位元记为 0,称为*零元素*,逆元记为$-a$. 并称为*负元素*.

群 G 中元素的个数记为$|G|$,称为 G 的*阶*. 称 G 为*有限群*,若其阶是有限的. 如果 A 和 B 是 G 的子集,则记

$$AB=\{ab:a\in A,b\in B\}\quad\text{或}\quad A+B=\{a+b:a\in A,b\in B\}.$$

例 12.11　(a) 整数集 $\mathbf{Z}$ 在加法下是一个阿贝尔群. 单位元是 0,$-a$ 是 a 在 $\mathbf{Z}$ 中的加法逆元.

(b) 非零有理数集 $\mathbf{Q}\backslash\{0\}$在乘法下构成一个阿贝尔群. 1 是单位元,$q/p$ 是有理数 p/q 的乘法逆元.

(c) 设 S 是 2×2 有理矩阵集合,并在其上定义了矩阵乘法. 则 S 不是一个群,因为逆元有时不存在. 但是,设 G 是行列式不为零的 2×2 矩阵的集合,那么 G 在乘法下是一个群,单位元是

$$I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\text{的逆元为}A^{-1}=\begin{bmatrix}d/|A| & -b/|A|\\ -c/|A| & a/|A|\end{bmatrix}$$

这不是一个阿贝尔群,因为矩阵乘法不可交换.

(d) 回顾 $\mathbf{Z}_m$ 指模 m 的整数,$\mathbf{Z}_m$ 在加法下构成群,但在乘法下不构成群. 但是设 $\mathbf{U}_m$ 是模 m 的一组简化剩余系,即由与 m 互素的那些数组成,那么 $\mathbf{U}_m$ 在乘法(模 m)下构成群. 例如,图 12-3 给出了 $\mathbf{U}_{12}=\{1,5,7,11\}$的乘法表

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

图 12-3

对称群 S_n

从集合$\{1,2,\cdots n\}$到自身的 1－1 映射 σ 称为置换，记为

$$\sigma=\begin{pmatrix}1 & 2 & 3\cdots n\\ j_1 & j_2 & j_3\cdots j_n\end{pmatrix}.$$

其中 $j_i=\sigma(i)$

所有置换的集合记为 S_n，共有 $n!=1\cdot 2\cdots n$ 个元素. S_n 中置换的复合和逆均在 S_n 中，并且单位函数 ε 也在 S_n 中，这样 S_n 在函数复合运算下构成群，我们称之为 n 阶对称群.

对称群 S_3 如下有 $3!=6$ 个元素：

$$\varepsilon=\begin{bmatrix}1 & 2 & 3\\1 & 2 & 3\end{bmatrix},\quad \sigma_2=\begin{bmatrix}1 & 2 & 3\\3 & 2 & 1\end{bmatrix},\quad \phi_1=\begin{bmatrix}1 & 2 & 3\\2 & 3 & 1\end{bmatrix},$$

$$\sigma_1=\begin{bmatrix}1 & 2 & 3\\1 & 3 & 2\end{bmatrix},\quad \sigma_3=\begin{bmatrix}1 & 2 & 3\\2 & 1 & 3\end{bmatrix},\quad \phi_2=\begin{bmatrix}1 & 2 & 3\\3 & 1 & 2\end{bmatrix}.$$

S_3 的乘法表见图 12－4.

	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ε	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ε	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ε	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ε	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ε
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ε	ϕ_1

图 12－4

MAP(A)，PERM(A)和 AUT(A)

设 A 是一非空集合，所有的函数(映射)$f:A\to A$ 组成的集合 MAP(A)在函数的复合下是半群，但它不是群，因为有些函数没有逆元. 但是所有的 A 到自身的 1－1 映射(称为置换)组成的 MAP(A)的子半群 PERM(A)在函数的复合下构成群.

进一步，设 A 含有某些几何和代数结构，例如 A 可以是一个图的顶点集合，或 A 是有序集或半群，那么所有 A 到自身的同构映射(称为 A 的自同态)所组成的集合AUT(A)在函数的复合下也构成群.

12.5　子群，正规子群和同态

设 H 是群G 的一个子集，那么 H 称为G 的子群，如果在 G 的运算下 H 本身也是群. 下面是判断子群的几条简单原则.

性质 12.5　群 G 的子集 H 是G 的子群，如果

(i) 单位元 $e\in H$；

(ii) 在 G 的运算下 H 封闭，即如果 $a,b\in H$，那么 $ab\in H$；

(iii) H 对逆元封闭，即如果 $a\in H$，那么 $a^{-1}\in H$.

每一个群 G 都以$\{e\}$和 G 自身为其子群，G 的其他子群都称为非平凡子群.

陪集

如果 H 是G 的子群且 $a\in G$，那么集合

$$Ha=\{ha:h\in H\}$$

称为 H 的*右陪集*.(类似地,aH 称为 H 的*左陪集*). 有下面的结论(见问题 12.17 和 12.19 中的证明).

定理 12.6 设 H 是群 G 的子群,那么右陪集 Ha 构成一个 G 的划分.

定理 12.7(拉格朗日) 设 H 是有限群 G 的子群. 则 H 的阶整除 G 的阶.

事实上,我们可以证明 G 中 H 的右陪集的数目(称为 H 在 G 中的指标)等于 G 中 H 的左陪集的数目,且两者都等于 $|G|$ 除以 $|H|$.

正规子群

定义 G 的一个子群 H 是*正规子群*,如果对于任意 $a\in G$,有 $a^{-1}Ha\subseteq H$. 等价地. H 是正规的,如果对于每个 $a\in G$ 有 $aH=Ha$ 即左陪集与右陪集相等.

注意阿贝尔群的每个子群都是正规的.

正规子群的重要性体现在下面的结论中(在问题 12.24 中证明).

定理 12.8 设 H 是群 G 的一个正规子群. 那么 H 的陪集在陪集乘法

$$(aH)(bH)=abH$$

下构成群,称为*商群*,记作 G/H.

设 G 中的运算是加法或者说 G 是加法式的,那么 G 的子群 H 的陪集形如 $a+H$. 而且,如果 H 是 G 的正规子群,那么 H 的陪集在下面陪集加法下形成群.

$$(a+H)+(b+H)=(a+b)+H$$

例 12.12 (a) 考虑前面讨论的 3 阶置换群 S_3. 集合 $H=\{\epsilon,\sigma_1\}$ 是 S_3 的一个子群. 其右陪集和左陪集分别为

右陪集	左陪集
$H=\{\epsilon,\sigma_1\}$,	$H=\{\epsilon,\sigma_1\}$,
$H\phi_1=\{\phi_1,\sigma_2\}$,	$\phi_1H=\{\phi_1,\sigma_3\}$,
$H\phi_2=\{\phi_2,\sigma_3\}$,	$\phi_2H=\{\phi_2,\sigma_2\}$.

易见右陪集与左陪集有所不同,故 H 不是 S_3 的正规子群.

(b) 考虑行列式不为 0 的 2×2 有理矩阵构成的群 G(见例 12.11(c)).

设 H 是右上角元素为 0 的矩阵构成的 G 的子集,即有下面形式

$$\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}$$

那么 H 是 G 的子群. 因为 H 在 G 的乘法下封闭具有逆元而且 $I\in H$. 但是 H 不是一个正规子群,例如

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}^{-1}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}=\begin{bmatrix} -1 & -4 \\ 1 & 3 \end{bmatrix}$$

不属于 H.

另外,设 K 是由行列式等于 1 的矩阵组成的 G 的子集. 可以证明 K 也是 G 的子群,并且对于任意矩阵 $X\in G$ 和 $A\in K$,有

$$\det(X^{-1}AX)=1.$$

因此 $X^{-1}AX\in K$,所以 K 是 G 的正规子群.

模 m 整数

考虑整数集在加法下构成的群 $\mathbf{Z}$,设 H 表示 5 的倍数的集合,也就是说,

$$H=\{\cdots,-10,-5,0,5,10,\cdots\}.$$

那么 H 是 $\mathbf{Z}$ 的子群(正规子群),$\mathbf{Z}$ 中 H 的陪集为

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

图 12-5

$$\overline{0}=0+H=H=\{\cdots,-10,-5,0,5,10,\cdots\},$$
$$\overline{1}=1+H=\{\cdots,-9,-4,1,6,11,\cdots\},$$
$$\overline{2}=2+H=\{\cdots,-8,-3,2,7,12,\cdots\},$$
$$\overline{3}=3+H=\{\cdots,-7,-2,3,8,13,\cdots\},$$
$$\overline{4}=4+H=\{\cdots,-6,-1,4,9,14,\cdots\}.$$

由定理 12.8，$\mathbf{Z}/H=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$在陪集加法下是一个群，它的加法表见图 12-5.

这个商群 $\mathbf{Z}/H$ 称为模 5 的整数通常记为 Z_5，类似地，对于任意正整数 n，存在商群 Z_n 即模 n 的整数.

循环子群

设 G 是任意群，a 是 G 中任一元素. 通常，我们定义 $a^0=e$ 和 $a^{n+1}=a^n\cdot a$. 显然，对于任何整数 m 和 n. $a^m\cdot a^n=a^{m+n}$，$(a^m)^n=a^{mn}$，a 的所有次幂

$$\cdots,a^{-3},a^{-2},a^{-1},e,a,a^2,a^3,\cdots$$

形成了一个 G 的子群，称为 a 生成的循环群，记为 $gp(a)$. 对于 a 的不同次幂，即 $a^r=a^s$ 且 $r>s$，有 $a^{r-s}=e(r-s>0)$. 满足 $a^m=e$ 的最小正整数 m 称为 a 的阶，记为$|a|$. 如果$|a|=m$，那么它的循环子群 $gp(a)$ 有 m 个元素

$$gp(a)=\{e,a,a^2,a^3,\cdots,a^{m-1}\}.$$

例如对于对称群 S_3 的元素 ϕ_1，有

$$\phi_1^1=\phi_1,\ \phi_1^2=\phi_2,\ \phi_1^3=\phi_2\cdot\phi_1=\varepsilon.$$

因此$|\phi_1|=3$，$gp(\phi_1)=\{e,\phi_1,\phi_2\}$. 注意$|\phi_1|$整除 S_3 的阶. 这对一般情况也成立，即对于群 G 中任何元素 a，我们可由拉格朗日定理 12.7，得 $gp(a)$的阶整除$|G|$. 如果群 G 中存在一元素 a 使得$G=gp(a)$，那么就称群 G 为循环群.

生成集和生成元

考虑群 G 的任意子集 A. 设 $gp(A)$表示 G 中所有元素 x 的集合，其中 x 是集合 $A\cup A^{-1}$ (A^{-1}表示 A 中所有元素的逆元组成的集合)中元素的积，即

$$gp(A)=\{x\in G:x=b_1b_2\cdots b_m,b_i\in A\cup A^{-1}\}.$$

那么 $gp(A)$是 G 的具有生成集 A 的一个子群. 特别地，如果 $G=gp(A)$，即 G 中每一个元素 g 都是 $A\cup A^{-1}$中元素的积，则称 A 生成群 G. 如果没有元素更少的集合生成 G，则称 A 是 G 的最小生成集. 例如，置换 $a=\sigma_1$ 和 $b=\phi_1$ 构成对称群 S_3（图 12-4）的一个最小生成集. 因为

$$\varepsilon=a^2,\ \sigma_1=a,\ \sigma_2=ab,\ \sigma_3=ab^2,\ \phi_1=b,\ \phi_2=b^2.$$

另外，S_3 不是循环群，因此它不能由一个元素生成.

同态

从群 G 到 G'的一个映射 f 称为同态，如果对任意的 $a,b\in G$，有

$$f(ab)=f(a)f(b).$$

如果 f 是 1-1 的，映上的，那么 f 叫做同构，称 G 和 G'同构，记作 $G\simeq G'$.

如果 $f:G\to G'$是一同态，那么 f 的核记为 $\mathrm{Ker}f$，是指 G 中像为 G'中的单位元 e'的元素构成的集合. 即

$$\mathrm{Ker}f=\{a\in G:f(a)=e'\}.$$

回顾 f 的像，记为 $f(G)$或 $\mathrm{Im}f$，即

$$\mathrm{Im}f=\{b\in G':存在\ a\in G\ 使得\ f(a)=b\}.$$

下面是群理论的一个基本定理(证明见问题 12.21).

定理 12.9 设 $f:G\to G'$为同态,核为 K,则 K 是 G 的正规子群,且商群 G/K 同构于 $f(G)$.

例 12.13 (a) 设 G 是实数在加法下构成的群,G'是正实数在乘法下构成的群. 由$f(a)=2^a$定义的映射 $f:G\to G'$是一同态,因为

$$f(a+b)=2^{a+b}=2^a2^b=f(a)f(b).$$

事实上,f 也是 1-1 和映上的,故 G 与 G'同构.

(b) 设 G 是非零复数在乘法下构成的群,G' 是非零实数在乘法下构成的群. 由 $f(z)=|z|$定义的映射 $f:G\to G'$是一同态,因为

$$f(z_1z_2)=|z_1z_2|=|z_1||z_2|=f(z_1)f(z_2).$$

f 的核 K 由单位圆$|z|=1$上的复数构成,因此 G/K 同构于 f 的像,即正实数在乘法下构成的群.

(c) 设 a 是群G 中任意元素,由 $f(n)=a^n$ 定义的函数 $f\mathbf{Z}\to G$ 是同态的,因为

$$f(m+n)=a^{m+n}=a^m\cdot a^n=f(m)\cdot f(n).$$

f 的像是由 a 生成的循环子群 $gp(a)$. 由定理 12.9 知

$$gp(a)\simeq \mathbf{Z}/K.$$

K 是 f 的核. 如果 $K=\{0\}$,那么 $gp(a)\simeq\mathbf{Z}$. 另外,如果 m 是 a 的阶,那么 $K=\{m$ 的倍数$\}$,因此 $gp(a)\simeq\mathbf{Z}_m$. 换句话说,任何循环群都同构于 $\mathbf{Z}$ 或者 $\mathbf{Z}_m$,即模 m 的整数的加法群.

12.6 环,整环和域

设 R 是定义了两个二元运算的非空集合,一个运算是加法(记为+),另一个运算是乘法(记为 *),那么 R 称为环,如果满足下面的公理

[$\mathbf{R}_1$] 对于任意 $a,b,c\in R$,有$(a+b)+c=a+(b+c)$.

[$\mathbf{R}_2$] 存在元素 $0\in R$,称为零元,使得对于每一个 $a\in R$ 有 $a+0=0+a=a$.

[$\mathbf{R}_3$] 对于每一个 $a\in R$,存在元素$-a\in R$,称为 a 的负元,使得 $a+(-a)=(-a)+a=0$.

[$\mathbf{R}_4$] 对于 $a,b\in R$,有 $a+b=b+a$.

[$\mathbf{R}_5$] 对于 $a,b,c\in R$,有$(ab)c=a(bc)$.

[$\mathbf{R}_6$] 对于任何 $a,b,c\in R$,有(i)$a(b+c)=ab+ac$; (ii)$(b+c)a=ba+ca$.

注意公理[$\mathbf{R}_1$]到[$\mathbf{R}_4$]可以简说成 R 关于加法构成阿贝尔群.

减法是通过 $a-b=a+(-b)$来定义的.

可以证明(见问题 12.29)对于任意的 $a\in R$ 有 $a\cdot 0=0\cdot a=0$.

R 的子集 S 是 R 的子环,如果 S 本身在 R 中运算下是环. 注意到,S 是 R 的子环只要 S 满足 (i) $0\in S$;(ii) 对任何 $a,b\in S$,有 $a-b\in S,ab\in S$.

特殊的环:整环和域

这部分内容定义了一些不同的环,包括整环和域.

R 称为交换环,如果对于每一个 $a,b\in R$,有 $ab=ba$.

R 称为有单位元 1 的环,如果对任何元素 $a\in R$. 元素 1 具有性质:$a\cdot 1=1\cdot a=a$. 此时,如果 a 有乘法逆元,即存在 $a^{-1}\in R$ 使得$aa^{-1}=a^{-1}a=1$,那么 a 称为一个单位.

R 称为零因子环,如果有非零元素 $a,b\in R$ 使得 $ab=0$. 此时,a 和 b 称为零因子.

定义 交换环 R 叫做整环,如果 R 没有零因子,即如果 $ab=0$ 则必有 $a=0$ 或$b=0$.

定义 有单位元 1(不等于 0)的交换环 R 叫做域,如果每一个非零元 $a(\in R)$是一个单位,即有乘法逆元.

一个域一定是整环,因为如果 $ab=0$ 且 $a\neq 0$,那么

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0.$$

需要注意的是域也可看做一交换环，其非零元在乘法下构成群.

例 12.14 (a) 对于通常的加法和乘法，整数集 $\mathbf{Z}$ 是整环(有单位元)的一个典型例子. $\mathbf{Z}$ 中的单位只有 1 和 -1，也就是说，$\mathbf{Z}$ 中没有其他元素有乘法逆元.

(b) 集合 $\mathbf{Z}_m = \{0,1,2,\cdots,m-1\}$ 在模 m 加法和乘法下是一个环，它称为模 m 整数环. 如果 m 是素数，则 $\mathbf{Z}_m$ 是域. 另一方面，如果 m 不是素数，那么 $\mathbf{Z}_m$ 有零因子. 例如，在环 $\mathbf{Z}_6$ 中，

$$2 \cdot 3 = 0 \quad 但 \quad 2 \neq 0 (\bmod 6),\ 3 \neq 0 (\bmod 6).$$

(c) 有理数集 $\mathbf{Q}$ 和实数集 $\mathbf{R}$ 各自在通常的加法和乘法下形成域.

(d) 设 M 表示 2×2 的整数矩阵或实矩阵的集合，那么 M 在矩阵加法和乘法下构成一个不可交换的零因子环. M 有单位元，即单位矩阵.

(e) 设 R 是任意环，那么 R 上的所有多项式组成的集合 $R[x]$ 在通常的多项式加法和乘法下构成环. 而且如果 R 是整环，那么 $R[x]$ 也是整环.

理想

环 R 的一个子集 J 称为理想，如果满足下列三个性质

(i) $0 \in J$.

(ii) 对于任意 $a,b \in J$，有 $a-b \in J$.

(iii) 对于任意 $r \in R$ 和 $a \in J$，有 $ra, ar \in J$.

首先注意 J 是 R 的一个子环，而且 J 是加法群 R 的一个子群(正规子群)因此陪集的集合

$$\{a + J : a \in R\}$$

构成 R 的一个划分.

理想的重要性体现在下面的定理中，这个定理类似于对于正规子群的定理 12.7.

定理 12.10 设 J 是环 R 的一个理想，那么陪集 $\{a+J : a \in R\}$ 在陪集运算下形成一个环.

$$(a+J)+(b+J) = a+b+J,\ (a+J)(b+J) = ab+J.$$

此环记为 R/J，称为商环.

现设 R 是一个交换环且有单位元 1，对于任何 $a \in R$，集合 $(a) = \{ra : r \in R\} = aR$ 是一个理想，它称为 a 生成的主理想. 如果 R 的每个理想都是主理想，那么 R 称为一个主理想环. 特别地，如果 R 又是一个整环，那么 R 称为主理想整环(PID).

例 12.15 (a) 考虑整数环 $\mathbf{Z}$，$\mathbf{Z}$ 中每一个理想 J 是主理想. 也就是说，对某个整数 m 有 $J = (m) = m\mathbf{Z}$. 因此 $\mathbf{Z}$ 是一个主理想整环(PID). 商群 $\mathbf{Z}_m = \mathbf{Z}/m$ 是模 m 整环. 尽管 $\mathbf{Z}$ 是整环(无零因子)，商环 $\mathbf{Z}_m$ 却可能有零因子. 例如 2 和 3 是 $\mathbf{Z}_6$ 的零因子.

(b) 设 R 是任一环，那么 $\{0\}$ 和 R 是理想. 特别地，如果 R 是域，那么 $\{0\}$ 和 R 是其仅有的主理想.

(c) 设 K 是一个域，那么 K 上的多项式环 $K[x]$ 是一个 PID(主理想整环)，另一方面，含有两个变量的多项式环 $K[x,y]$ 不是一个 PID.

(d) 设 M 是 2×2 整数矩阵环，设 J 为形式如下的所有矩阵组成的集合

$$\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}.$$

注意 (i) $0 \in J$. (ii) 对任何 $a,b \in J$，有 $a-b \in J$. (iii) 对任何 $r \in M$ 和 $a \in J$，有 $ra \in J$；即 $RJ \subseteq J$，但 $JR \not\subseteq J$，因此 J 不是一个理想(称之为左理想.)

环同态

从环 R 到环 R' 的一个映射 f 称为一个环同态或简称同态，如果对任意的 $a,b \in R$，有

$$f(a+b) = f(a) + f(b),\quad f(ab) = f(a)f(b).$$

另外,如果 f 是 1-1 和映上的,则称 f 为同构,R 和 R' 称为同构,记为 $R\simeq R'$.

如果 $f:R\to R'$ 是一同态,那么 f 的核记为 $\mathrm{Ker}f$,是指 R 中以 R' 的零元素为像的元素的集合,即

$$\mathrm{Ker}f=\{r\in R:f(r)=0\}.$$

下面的定理(类似于群的定理 12.9)是环理论的一个基本定理.

定理 12.11 设 $f:R\to R'$ 是一个核为 K 的环同态,那么 K 是 R 中的一个理想,商群 R/K 与 $f(R)$ 同构.

整环上的整除

现设 D 是一整环,说 b 整除 a,如果对于某个 $c\in D$ 有 $a=bc$. 元素 $u\in D$ 称为一个单位,如果 u 整除 1,即如果 u 有一个乘法逆元. 元素 $b\in D$ 称为 $a\in D$ 的伴元,如果 $b=ua$ 对于某个单位 $u\in D$. 一个非单位 $p\in D$ 称为不可约的,如果 $p=ab$ 推出 a 或 b 是一个单位.

整环 D 称为一个惟一分解环(UFD),如果每个非单位 $a\in D$ 可以惟一地写成不可约元素的积(不计伴元和顺序).

例 12.16 (a) 整数环 **Z** 是惟一分解环的一个典型例子. **Z** 的单位是 1 和 -1. $n\in\mathbf{Z}$ 的仅有伴元是 n 和 $-n$. **Z** 的不可约元素是素数.

(b) 集合 $D=\{a+b\sqrt{13}:a,b$ 为整数$\}$ 是一整环,D 的单位是 ±1, $18\pm5\sqrt{13}$ 和 $-18\pm5\sqrt{13}$,元素 2, $3-\sqrt{13}$ 和 $-3-\sqrt{13}$ 是 D 中的不可约元素. 注意

$$4=2\cdot2=(3-\sqrt{13})(-3-\sqrt{13}).$$

因此 D 不是惟一分解环(见问题 12.99).

12.7 域上的多项式

本节主要研究以整环或域中元素为系数的多项式. 特别地,我们将证明域 K 上的多项式有许多和整数一样的性质.

基本的定义

设 K 是一个整环或域,严格地说,K 上的多项式 f 是 K 中元素的无限序列,其中有限个元素不为零,即

$$f=(\cdots,0,a_n,\cdots,a_1,a_0)\quad 或\quad f(t)=a_nt^n+\cdots+a_0.$$

其中 t 作为一个不定元. a_k 称为 f 的第 k 个系数. 满足 $a_n\neq0$ 的最大的 n 称为多项式的次数,记为 $\deg(f)=n$. 我们也称 a_n 是 f 的首项系数. 且如果 $a_n=1$,称 f 是一标准多项式;另一方面,如果 f 的每个系数都为零,则 f 称为零多项式,记为 $f\equiv0$. 零多项式的次数没有定义.

设 $K[t]$ 是 K 上所有多项式 $f(t)$ 的集合. $K[t]$ 中加法和乘法定义如下. 设

$$f(t)=a_nt^n+\cdots+a_0,\ g(t)=b_mt^m+\cdots+b_0.$$

那么和 $f+g$ 是指 f 和 g 中相应系数相加所得的多项式,即如果 $m\leqslant n$,那么

$$f(t)+g(t)=a_nt^n+\cdots+(a_m+b_m)t^m+\cdots+(a_1+b_1)t+(a_0+b_0).$$

f 和 g 的积是多项式

$$f(t)g(t)=(a_nb_m)t^{n+m}+\cdots+(a_1b_0+a_0b_1)t+(a_0b_0).$$

即

$$f(t)g(t)=c_{n+m}t^{n+m}+\cdots+c_1t+c_0,\ 其中$$

$$c_k=\sum_{i=0}^{k}a_ib_{k-i}=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0.$$

数量集 K 可看做是 $K[t]$ 的一个子集,特别地将数量 $a_0\in K$ 与多项式

$$f(t)=a_0\quad 或\quad a_0=(\cdots,0,0,a_0)$$

视为等同.加法运算和乘法运算可如下定义

$$(\cdots,0,a_0)+(\cdots,0,b_0)=(\cdots,0,a_0+b_0),\ (\cdots,0,a_0)\cdot(\cdots,0,b_0)=(\cdots,0,a_0b_0).$$

因此由 $\Psi(a_0)=a_0$ 定义的映射 $\Psi:K\to K[t]$ 是将 K 嵌入 $K[t]$ 的一个同构映射.

定理 12.12 设 K 是一整环. $K[t]$ 在多项式加法和乘法下是一有单位元为 1 的交换环.

下面这个简单的引理对以后的证明有很大作用.

引理 12.13 设 f 和 g 是整环 K 上的多项式,那么

$$\deg(fg)=\deg(f)+\deg(g).$$

证明可由多项式积的定义直接得到.即设 $f(x)=a_nt^n+\cdots+a_0$ 和 $g(t)=b_mt^m+\cdots+b_0$,其中 $a_n\neq0,b_m\neq0$,那么

$$f(t)g(t)=a_nb_mt^{m+n}+\text{较低次数的式子}.$$

又因为 K 是一个整环,没有零因子,$a_nb_m\neq0$ 因此,

$$\deg(fg)=m+n=\deg(f)+\deg(g).$$

引理得证.

下面列出了多项式的许多性质(回顾一个多项式 g 整除 f,如果存在多项式 h,使得 $f(t)=g(t)h(t)$):

性质 12.14 设 K 是一个整环,f 和 g 是 K 上的多项式.

(i) $K[t]$ 是一整环.

(ii) $K[t]$ 的单位是 K 的单位.

(iii) 如果 g 整除 f,那么 $\deg(g)\leqslant\deg(f)$.

(iv) 如果 g 整除 f,f 整除 g,那么 $f(t)=kg(t)$,其中 k 是 K 的一个单位.

(v) 如果 d 和 d' 均为标准多项式,且使得 d 整除 d',d' 整除 d,那么 $d=d'$.

带余除法和多项式的根

这里我们讨论以域 K 中元素为系数的多项式 $f(t)$ 的根.回顾 $a\in K$ 是 $f(t)$ 的一个根,如果 $f(a)=0$.首先从一个重要的定理开始,它类似于整数集 $\mathbf{Z}$ 上的相应定理.

定理 12.15(带余除法) 设 $f(t)$ 和 $g(t)$ 是域 K 上的多项式且

$g(t)\neq0$,那么存在多项式 $q(t)$ 和 $r(t)$ 使得

$$f(t)=q(t)g(t)+r(t).$$

其中 $r(t)\equiv0$ 或者 $\deg(r)<\deg(g)$

上述定理(证明见问题 12.39)规范了"长除法"的过程,多项式 $q(t)$ 称为商式多项式 $r(t)$ 称为余式.

推论 12.16(剩余定理) 假设 $f(t)$ 被 $g(t)=t-a$ 除,那么余式是 $f(a)$.

证明可由带余除法得到.即用 $t-a$ 除 $f(t)$ 得到

$$f(t)=q(t)(t-a)+r(t).$$

其中 $\deg(r)<\deg(t-a)=1$.因此 $r(t)=r$ 是一个数量,用 $t=a$ 代入上述方程得

$$f(a)=q(a)(a-a)+r=q(t)\cdot0+r=r.$$

因此余数是 $f(a)$.

推论 12.16 还告诉我们 $f(a)=0$ 当且仅当余式 $r=r(t)\equiv0$.于是有下面的推论.

推论 12.17(因式定理) 数量 $a\in K$ 是 $f(t)$ 的一个根当且仅当 $t-a$ 是 $f(t)$ 的一个因式.

下面的定理告诉我们一个多项式可能的根的数目.

定理 12.18 假设 $f(t)$ 是域 K 上的一个多项式且 $\deg(f)=n$.那么 $f(t)$ 至多有 n 个根.

下面的定理是求整系数多项式有理根的一个主要方法.

定理 12.19 假设有理数 p/q(最简形式)是多项式

$$f(t)=a_nt^n+\cdots+a_1t+a_0$$

的一个根，其中所有的系数 $a_n,\cdots,a_1,a_0$ 是整数. 那么 p 整除常数项 a_0，q 整除首项系数 a_n. 特别地，如果 $c=p/q$ 是一整数，那么 c 整除常数项 a_0.

例 12.17 (a) 设 $f(t)=t^3+t^2-8t+4$，假设 $f(t)$ 有一个有理根，求出 $f(t)$ 的所有根.

因为首项系数是 1，$f(t)$ 的有理根必在 $+1,\pm 2,\pm 4$ 中，$f(1)\neq 0$ 且 $f(-1)\neq 0$，由综合除法，或用 $t-2$ 除，得到

$$\begin{array}{r|rrrr} 2 & 1 & +1 & -8 & +4 \\ & & 2 & +6 & -4 \\ \hline & 1 & +3 & -2 & +0 \end{array}$$

因此 $t=2$ 是一个根，$f(t)=(t-2)(t^2+3t-2)$. 对 $t^2-3t-2=0$ 用求根公式，我们得到 $f(t)$ 的下列根

$$t=2,\ t=(-3+\sqrt{17})/2,\ t=(-3-\sqrt{17})/2.$$

(b) 设 $h(t)=t^4-2t^3+11t-10$，求出 $h(t)$ 的所有实根，假设其中有两个整数根.

整数根必在 $\pm 1,\pm 2,\pm 5,\pm 10$ 之中，由综合除法（或用 $t-1$ 除再用 $t+2$ 除）我们得到

$$\begin{array}{r|rrrrr} 1 & 1 & -2 & -0 & +11 & -10 \\ & & 1 & -1 & -1 & +10 \\ \hline -2 & 1 & -1 & -1 & +10 & +0 \\ & & -2 & +6 & -10 & \\ \hline & 1 & -3 & +5 & -0 & \end{array}$$

因此 $t=1$ 和 $t=-2$ 是两个整数根，$h(t)=(t-1)(t+2)(t^2-3t+5)$. 由求根公式知 $t^2+3t+5=0$ 无实根. 因此，$t=1$ 和 $t=-2$ 是 $h(t)$ 仅有的实根.

$K[t]$ 作为 PID 和 UFD

定理 12.20 域 K 上的多项式环 $K[t]$ 是一个主理想整环(PID). 如果 J 是 $K[t]$ 中的一个理想，那么存在惟一的标准多项式 d 生成 J，也就是说 J 中每一个多项式都是 d 的倍数.

定理 12.21 设 f 和 g 是 $K[t]$ 中的多项式，那么存在一个惟一的标准多项式 d 使得

(i) d 既整除 f 又整除 g.

(ii) 如果 d' 整除 f 和 g，那么 d' 整除 d.

在上面定理中的多项式 d 称为 f 和 g 的*最大公因式*，记作 $d=\gcd(f,g)$. 如果 $d=1$，那么 f 和 g 称为*互素*.

推论 12.22 设 d 是 f 和 g 的最大公因式，那么存在多项式 m 和 n 使得 $d=mf+ng$. 特别地，如果 f 和 g 互素，那么存在多项式 m 和 n 使得 $mf+ng=1$.

多项式 $p\in K[t]$ 称为不可约的，如果 p 不是数量且 $p=fg$ 可推出 f 或 g 是一个数量. 换句话说，p 不可约. 如果它的所有因式都是它的伴元(数量倍数).

引理 12.23 设 $p\in K[t]$ 是不可约的，如果 p 整除 $K[t]$ 中多项式 f 和 g 的乘积 fg，那么 p 整除 f 或 p 整除 g. 更一般地，如果 p 整除 n 个多项式的积 $f_1f_2\cdots f_n$，那么 p 整除它们当中的一个.

下面的定理指出一个域上的多项式形成一个惟一分解环(UFD).

定理 12.24(惟一分解定理) 设 f 是 $K[t]$ 中一个非零多项式. 那么 f 除顺序外可惟一写成一个积

$$f=kp_1p_2\cdots p_n.$$

其中 $k\in K$，p_i 是 $K[t]$ 中的标准不可约多项式.

代数基本定理

下面这个定理的证明超出了本书的范围

代数基本定理　复数域 **C** 上的任意非零多项式 $f(t)$ 都有一个复根，因此 $f(t)$ 除顺序外可惟一写成积

$$f(t)=k(t-r_1)(t-r_2)\cdots(t-r_n).$$

其中 k 和 r_i 是复数且 $\deg(f)=n$.

上面的定理在实数域 **R** 上可能不正确. 例如，$f(t)=t^2+1$ 是实数域 **R** 上的一个多项式，但 $f(t)$ 没有实根.

定理 12.25　设 $f(t)$ 是实数域 **R** 上的一个多项式，并且假设复数 $z=a+bi$，$b\neq 0$，是 $f(t)$ 的一个根，那么复数 z 的共轭 $\bar{z}=a\quad bi$ 也是 $f(t)$ 的一个根. 因此，

$$c(t)=(t-z)(t-\bar{z})=t^2-2at-a^2+b^2$$

是 $f(t)$ 的一个因式.

定理 12.26　设 $f(t)$ 是实数域 **R** 上的一个非零多项式，那么 $f(t)$ 可以除顺序外惟一写成积

$$f(t)=kp_1(t)p_2(t)\cdots p_m(t).$$

其中 $k\in R$ 且 pj 为 1 次或 2 次的实标准多项式.

例 12.18　设 $f(t)=t^4-3t^3+6t^2+25t-39$. 已知 $t=2+3i$ 是一个根，求 $f(t)$ 的所有根.

既然 $2+3i$ 是一个根，那么 $2-3i$ 也是一个根，$c(t)=t^2-4t-13$ 就是 $f(t)$ 的一个因式. $f(t)$ 被 $c(t)$ 除得

$$f(t)=(t^2-4t+13)(t^2+t-3).$$

对 $t^2+t-3=0$ 用求根公式得 $f(t)$ 的其他根，即 $f(t)$ 的四个根为

$$t=2+3i,\ t=2-3i,\ t=(-1+\sqrt{13})/2,\ t=(-1-\sqrt{13})/2.$$

问题与解答

运算和半群

12.1　考虑正整数集 **N**，设 $*$ 表示 **N** 上求最小公倍数的运算(lcm).

(a) 求 $4*6$，$3*5$，$9*18$ 和 $1*6$.

(b) $(\mathbf{N},*)$ 是半群吗？可交换吗？

(c) 求 $*$ 的单位元.

(d) **N** 中哪些元素有逆元，是什么？

解 ☞　(a) 因为 $x*y$ 是指 x 和 y 的最小公倍数，有：

$$4*6=12,\ 3*5=15,\ 9*18=18,\ 1*6=6.$$

(b) 在数论中将证明 $(a*b)*c=a*(b*c)$，即运算 lcm 是可结合的. $a*b=b*a$ 即运算 lcm 是可交换的，因此 $(\mathbf{N},*)$ 是一个交换半群.

(c) 整数 1 是单位元，因为对于任何整数 a，$\mathrm{lcm}(1,a)=a$. 即对于任何整数 $a\in\mathbf{N}$ 有 $1*a=a*1=a$.

(d) 因为 $\mathrm{lcm}(a,b)=1$ 当且仅当 $a=1$ 和 $b=1$，所以惟一有逆元的元素就是 1，它的逆元就是它本身.

12.2　考虑有理数集 **Q**，设 $*$ 是 **Q** 上的运算，定义为

$$a*b=a+b-ab.$$

(a) 求 $3*4$，$2*(-5)$ 和 $7*\frac{1}{2}$.

(b) $(Q,*)$ 是半群吗？可交换吗？

(c) 求 $*$ 的单位元.

(d) Q中有元素有逆元吗？是什么？

解 ☞ (a) $3*4=3+4-3\cdot(4)=3+4-12=-5$.

$2*(-5)=2+(-5)-2(-5)=2-5+10=7$.

$7*\frac{1}{2}=7+\frac{1}{2}-7\left(\frac{1}{2}\right)=4$.

(b) 有

$$\begin{aligned}(a*b)*c&=(a+b-ab)*c\\&=(a+b-ab)+c-(a+b-ab)c\\&=a+b-ab+c-ac-bc+abc\\&=a+b+c-ab-ac-bc+abc.\\a*(b*c)&=a*(b+c-bc)\\&=a+(b+c-bc)-a(b+c-bc)\\&=a+b+c-ab-ac-bc+abc.\end{aligned}$$

因此 $*$ 是可结合的且 $(Q,*)$ 是一半群，而且

$$a*b=a+b-ab=b+a-ba=b*a.$$

因此 $(Q,*)$ 是一交换半群.

(c) 元素 e 是单位元，如果对于每一个 $a\in Q$，$a*e=a$. 运算如下

$$a*e=a,\ a+e-ae=a,\ e-ea=0,\ e(1-a)=0,\ e=0.$$

于是，0 是单位元.

(d) 为了使 a 有一个逆元 x，我们必有 $a*x=0$，因为由(c)可知 0 是单位元，运算如下

$$a*x=0,\ a+x-ax=0,\ a=ax-x,\ a=x(a-1),\ x=a/(a-1).$$

因此如果 $a\neq 1$，那么 a 有逆元 $a/(a-1)$.

12.3 设 S 是一半群，单位元为 e. 设 b 和 b' 是 a 的逆元，证明 $b=b'$，即逆元如果存在就惟一.

证明 ☞ 有

$$b*(a*b')=b*e=b,\ (b*a)*b'=e*b'=b'.$$

因为 S 是可结合的，$(b*a)*b'=b*(a*b')$；故 $b=b'$.

12.4 检验正整数集 **N** 的下列六个子集在乘法运算下是否封闭：

(a) $A=\{0,1\}$.　　　　　　　　　(b) $B=\{1,2\}$.

(c) $C=\{x:x$ 是素数$\}$.　　　　　(d) $D=\{2,4,6,\cdots\}=\{x:x$ 是偶数$\}$.

(e) $E=\{1,3,5,\cdots\}=\{x:x$ 是奇数$\}$.　(f) $F=\{2,4,8,\cdots\}=\{x:x=2^n,n\in N\}$.

六个集合中哪些在加法运算下封闭？

解 ☞ (a) 有：

$$0\cdot 0=0,\ 0\cdot 1=0,\ 1\cdot 0=0,\ 1\cdot 1=1.$$

因此 A 在乘法下封闭.

(b) 因为 $2\cdot 2=4\notin B$，所以集合 B 在乘法下不封闭.

(c) 注意到 2 和 3 是素数，而 $2\cdot 3=6$ 不是素数，因此 C 在乘法下不封闭.

(d) 偶数的积仍是偶数，因此 D 在乘法下封闭.

(e) 奇数的积仍是奇数，因此 E 在乘法下封闭.

(f) 因为 $2^r\cdot 2^s=2^{r+s}$，F 在乘法下封闭.

因为两个偶数的和仍是偶数，所以集合 D 在加法下封闭. 然而，其他任何一集合在加法下都不封闭，例如

$$1+1=2\notin A,\ 3+5=8\notin C,\ 2+4=6\notin F,$$
$$1+2=3\notin B,\ 1+3=4\notin E.$$

12.5 设 $S=\mathbf{N}\times\mathbf{N}$，$*$ 是 S 上的运算，定义为 $(a,b)*(a',b')=(aa',bb')$.

(a) 证明 $*$ 是可结合的(因此 S 是一半群).

(b) 由 $f(a,b)=a/b$ 来定义 $f:(S,*)\to(\mathbf{Q},\times)$. 证明 f 是一同态映射.

(c) 求由同态映射 f 决定的同余关系，即 $x\sim y$，如果 $f(x)=f(y)$(见定理 12.4).

(d) 描述 $S/\sim$，$S/\sim$ 有单位元吗？有逆元吗？

解 ☞ 设 $x=(a,b)$，$y=(c,d)$，$z=(e,f)$.

(a) 有

$$(xy)z=(ac,bd)*(e,f)=[(ac)e,(bd)f],$$
$$x(yz)=(a,b)*(ce,df)=[a(ce),b(df)].$$

因为 a,b,c,d,e,f 是正整数，$(ac)e=a(ce)$，$(bd)f=b(df)$，

因此 $(xy)z=x(yz)$，$*$ 是可结合的，故 $(S,*)$ 是一半群.

(b) 有

$$f(x*y)=f(ac,bd)=(ac)/(bd)=(a/b)(c/d)=f(x)f(y).$$

因此 f 是一同态映射.

(c) 假设 $f(x)=f(y)$，那么

$$\frac{a}{b}=\frac{c}{d}，因此\ ad=bc.$$

因此 f 就通过如果 $ad=bc$，那么 $(a,b)\sim(c,d)$ 定义了 S 上的同余关系.

(d) f 的像是正有理数集 $\mathbf{Q}^+$，由定理 12.3，知 $S/\sim$ 同构于 $\mathbf{Q}^+$. 因此 $S/\sim$ 有单位元，并且每一个元素都有逆元.

12.6 设 $S=\mathbf{N}\times\mathbf{N}$，$*$ 是 S 上的运算定义为

$$(a,b)*(a',b')=(a+a',b+b').$$

(a) 证明 $*$ 是可结合的(因此 S 是一半群).

(b) 由 $f(a,b)=a-b$ 定义 $f:(S,*)\to(\mathbf{Z},+)$，证明 f 是一同态.

(c) 求由同态映射 f 决定的同余关系，即 $x\sim y$，如果 $f(x)=f(y)$(见定理 12.4).

(d) 描述 $S/\sim$，$S/\sim$ 有单位元吗？它有逆元吗？

解 ☞ 假设 $x=(a,b)$，$y=(c,d)$，$z=(e,f)$.

(a) 有

$$(xy)z=(a+c,b+d)*(e,f)=[(a+c)+e,(b+d)+f].$$
$$x(yz)=(a,b)*(c+e,d+f)=[a+(c+e),b+(d+f)].$$

由于 a,b,c,d,e,f 是正整数，

$$(a+c)+e=a+(c+e),\ (b+d)+f=b+(d+f).$$

因此 $(xy)z=x(yz)$，$*$ 是可结合的，即 $(S,*)$ 是一半群.

(b) 有

$$f(x*y)=f(a+c,b+d)=(a+c)-(b+d)$$
$$=(a-b)+(c-d)=f(x)f(y).$$

因此 f 是一同态.

(c) 设 $f(x)=f(y)$，那么 $a-b=c-d$，因此 $a+d=b+d$. 这样 f 决定的 S 上的同余关系定义为

$$(a,b)\sim(c,d)，若\ a+d=b+c.$$

(d) f 的像是 $\mathbf{Z}$ 的全部. 因为每一个整数是两个正整数的差. 因此，由定理 12.3，$S/\sim$ 同构于 $\mathbf{Z}$. 因此 $S/\sim$ 有单位元，且每一个元素都有(加法)逆元.

12.7 证明定理 12.1：假设 $*$ 是集合 S 上的一个可结合的运算，那么任何积 $a_1*a_2\cdots*a_n$ 可不加括号，即所有可能的积相等.

证明 ☞ 对 n 用归纳法. 因为 n 是可结合的，定理满足 $n=1,2$ 和 3. 假设 $n\geq4$. 用记号：

$$(a_1a_2,\cdots a_n)=(\cdots((a_1a_2)a_3)\cdots)a_n \quad 和 \quad [a_1a_2\cdots a_n]=任何积$$

我们将证明了 $[a_1a_2\cdots a_n]=(a_1a_2\cdots a_n)$，从而所有的这些积相等. 因为 $[a_1a_2\cdots a_n]$ 表示某个积，存在 $r<n$，使得 $[a_1a_2\cdots a_n]=[a_1a_2\cdots a_r][a_{r+1}\cdots a_n]$. 因此，由归纳法得，

$$[a_1a_2\cdots a_n]=[a_1a_2\cdots a_r][a_{r+1}\cdots a_n]=[a_1a_2\cdots a_r](a_{r+1}\cdots a_n)$$
$$=[a_1\cdots a_r]((a_{r+1}\cdots a_{n-1})a_n)=([a_1\cdots a_r](a_{r+1}\cdots a_{n-1}))a_n$$
$$=[a_1\cdots a_{n-1}]a_n=(a_1\cdots a_{n-1})a_n=(a_1a_2\cdots a_n)$$

因此定理得证.

12.8 证明定理 12.4：设 $f:S\to S'$ 是一半群同态. 如果 $f(a)=f(b)$，设 $a\sim b$，那么(i) $\sim$ 是一个同余关系，(ii) $S/\sim$ 同构于 $f(S)$.

证明 ☞ (i) 首先我们证明 $\sim$ 是一等价关系. 由于 $f(a)=f(a)$，有 $a\sim a$. 如果 $a\sim b$，那么 $f(a)=f(b)$ 或 $f(b)=f(a)$，因此 $b\sim a$. 最后，如果 $a\sim b, b\sim c$，那么 $f(a)=f(b)$，$f(b)=f(c)$，因此 $f(a)=f(c)$，因此 $a\sim c$. 即 $\sim$ 是一等价关系. 假设 $a\sim a'$，$b\sim b'$，那么 $f(a)=f(a')$ 且 $f(b)=f(b')$，因为 f 是一同态.

$$f(ab)=f(a)f(b)=f(a')f(b')=f(a'b').$$

所以 $ab\sim a'b'$. 即 $\sim$ 是一同余关系.

(ii) 定义 $\Psi:S/\sim\to f(S)$，$\Psi([a])=f(a)$. 只要证明：(1) Ψ 是有定义的，即 $\Psi([a])\in f(S)$ 且如果 $[a]=[b]$，那么 $f([a])=f([b])$. (2) Ψ 是一个同构，即 Ψ 是同态，且 1－1 映上的.

(1) 证明 Ψ 是有定义，设 $\Psi([a])=f(a)$. 因为 $a\in S$，有 $f(a)\in f(S)$. 因此 $\Psi([a])\in f(S)$. 现设 $[a]=[b]$，那么 $a\sim b$ 且 $f(a)=f(b)$，因此

$$\Psi([a])=f(a)=f(b)=\Psi([b]).$$

即 Ψ 是有定义的.

(2) 证明 Ψ 是一同构映射：因为 f 是一同态，

$$\Psi([a][b])=\Psi[ab]=f(ab)=f(a)f(b)=\Psi([a])\Psi([b]).$$

因此，Ψ 是一同态. 假设 $\Psi([a])=\Psi([b])$，那么 $f(a)=f(b)$. 于是 $a\sim b$，这样 $[a]=[b]$ 并且 Ψ 是 1－1 的. 最后，设 $y\in f(S)$，那么对于某个 $a\in S$，有 $f(a)=y$. 因此 $\Psi([a])=f(a)=y$. 所以 Ψ 是映上的，故 Ψ 是同构映射.

群

12.9 考虑对称群 S_3，它的乘法表见图 12－4.

(a) 求 S_3 中每一个元素的阶和生成群.

(b) 求 S_3 的所有子群的个数.

(c) 设 $A=\{\sigma_1,\sigma_2\}$，$B=\{\phi_1,\phi_2\}$. 求 AB、σ_3A 和 $A\sigma_3$.

(d) 设 $H=gp(\sigma_1)$，$K=gp(\sigma_2)$，证明 HK 不是 S_3 的子群.

(e) S_3 是循环群吗？

解 ☞ (a) 共有 6 个元素：(1)ε，(2)σ_1，(3)σ_2，(4)σ_3，(5)ϕ_1，(6)ϕ_2，找出每个元素 x 的幂，使得 $x^n=\varepsilon$，那么 $|x|=n$，$gp(x)=\{\varepsilon,x,x^2,\cdots x^{n-1}\}$. 注意 $x^1=x$ 故当 $x\neq\varepsilon$ 时，只需从 $n=2$ 开始.

(1) $\varepsilon^1=\varepsilon$；因此 $|\varepsilon|=1$，$g(\varepsilon)=\{\varepsilon\}$.

(2) $\sigma_1^2=\varepsilon$；因此 $|\sigma_1|=2$，$gp(\sigma_1)=\{\varepsilon,\sigma_1\}$.

(3) $\sigma_2^2=\varepsilon$；因此 $|\sigma_2|=2$，$gp(\sigma_2)=\{\varepsilon,\sigma_2\}$.

(4) $\sigma_3^2=\varepsilon$；因此 $|\sigma_3|=2$，$gp(\sigma_3)=\{\varepsilon,\sigma_3\}$.

(5) $\phi_1^2=\phi_2$，$\phi_1^3=\phi_2\phi_1=\varepsilon$；因此 $|\phi_1|=3$，$gp(\phi_1)=\{\varepsilon,\phi_1,\phi_2\}$.

(6) $\phi_2^2=\phi_1$，$\phi_2^3=\phi_1\phi_2=\varepsilon$；因此 $|\phi_2|=3$，$gp(\phi_2)=\{\varepsilon,\phi_2,\phi_1\}$.

(b) 首先，$H_1=\{e\}$，$H_2=S_3$ 是 S_3 的子群. S_3 的其他子群的阶必为 2 或 3，因为它们的阶一定整除 $S_3=6$. 因为 2 和 3 是素数，这些子群一定是循环的(见问题 12.65)，因此必定出现在(a)中，于是 S_3 其他的子群是

$$H_3=\{e,\sigma_1\},\ H_4=\{e,\sigma_2\},\ H_5=\{e,\sigma_3\},\ H_6=\{e,\phi_1,\phi_2\}.$$

所以 S_3 有 6 个子群.

(c) 用 B 中每一个元素去乘 A 中每一个元素

$$\sigma_1\phi_1=\sigma_2,\ \sigma_1\phi_2=\sigma_3,\ \sigma_3\phi_1=\sigma_1,\ \sigma_2\phi_2=\sigma_1.$$

因此 $AB=\{\sigma_1,\sigma_2,\sigma_3\}$.

用 A 中每一个元素乘 σ_3

$$\sigma_3\sigma_1=\phi_1,\ \sigma_3\sigma_2=\phi_2.$$

因此 $\sigma_3A=\{\phi_1,\phi_2\}$

用 σ_3 乘 A 中每一个元素

$$\sigma_1\sigma_3=\phi_2,\ \sigma_2\sigma_3=\phi_1$$

因此 $A\sigma_3=\{\phi_1,\phi_2\}$

(d) $H=\{e_1\sigma_1\}$, $K=\{e_1\sigma_2\}$，那么 $HK=\{e_1,\sigma_1\sigma_2,\phi_1\}$不是 S_3 的子群，因为 HK 有 4 个元素.

(e) 因为 S_3 中没有任何一个元素能生成 S_3，所以 S_3 不是循环群.

12.10　考虑在模 7 乘法下的群 $G=\{1,2,3,4,5,6\}$.

(a) 求 G 的乘法表.

(b) 求 $2^{-1},3^{-1},6^{-1}$.

(c) 求 2 和 3 的阶及由它们生成的子群.

(d) G 是循环群吗?

解 ☞　(a) 为了在 G 中求 $a*b$，必须求积 ab 被 7 除的余数. 例如，$5\cdot 6=30$ 除以 7 后得余数为 2，因此 $5*6=2$. G 的乘法表见图 12-6

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

图 12-6

(b) 首先 1 是 G 的单位元，回顾 a^{-1} 是 G 中的元素使得 $aa^{-1}=1$.

因此 $2^{-1}=4, 3^{-1}=5, 6^{-1}=6$.

(c) 我们有 $2^1=2, 2^2=4$，但 $2^3=1$，所以 $|2|=3$, $gp(2)=\{1,2,4\}$. 我们有 $3^1=3, 3^2=2, 3^3=6, 3^4=4, 3^5=5, 3^6=1$，所以 $|3|=6$, $gp(3)=G$.

(d) G 是循环的. 因为 $G=gp(3)$.

12.11　设 G 是模 15 的一个简化剩余系，如

$$G=\{1,2,4,7,8,11,13,14\}$$

(在 1 与 15 之间的与 15 互素的数的集合)，那么 G 在模 15 乘法下是一个群.

(a) 求 G 的乘法表.

(b) 求 $2^{-1},7^{-1},11^{-1}$.

(c) 求由 2,7 和 11 生成的子群和它们的阶.

(d) G 是循环的吗?

解 ☞　(a) 为了在 G 中求 $a*b$，必须要求积 ab 除 15 的余数，乘法表见图 12-7.

(b) 整数 r 和 s 互逆，如果 $r*s=1$. 因此 $2^{-1}=8, 7^{-1}=13, 11^{-1}=11$.

(c) 我们有 $2^2=4, 2^3=8, 2^4=1$. 故 $|2|=4$, $gp(2)=\{1,2,4,8\}$. 而 $7^2=4, 7^3=4*7=13, 7^4=13*7=1$，所有 $|7|=4$, $gp(7)=\{1,4,7,13\}$. 最后 $11^2=1$，故 $|11|=2$ 且 $gp(11)=\{1,11\}$.

(d) 因为 G 中没有元素生成它，所以 G 不是循环群.

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

图 12-7

12.12 设 σ 和 τ 是对称群 S_6 的两个元素，且

$$\sigma=\begin{bmatrix}1&2&3&4&5&6\\3&1&5&4&6&2\end{bmatrix},\ \tau=\begin{bmatrix}1&2&3&4&5&6\\5&3&1&6&2&4\end{bmatrix}.$$

求：$\tau\sigma,\sigma\tau,\sigma^2$ 和 σ^{-1}.（因为 τ 和 σ 是函数，$\tau\sigma$ 意思是先运算 σ，然后计算 τ.）

解☞ 在 1，2，…，6 上先作用 σ，然后再 τ，见图 12－8(a)；在 1，2，…6 上先作用 τ，然后作用 σ 见图 12－8(b). 在 1，2，…6 上连续两次作用 σ 见图 12－8(c). 因此

$$\tau\sigma=\begin{bmatrix}1&2&3&4&5&6\\1&5&2&6&4&3\end{bmatrix},\ \sigma\tau=\begin{bmatrix}1&2&3&4&5&6\\6&5&3&2&1&4\end{bmatrix},\ \sigma^2=\begin{bmatrix}1&2&3&4&5&6\\5&3&6&4&2&1\end{bmatrix}.$$

我们将 σ 的最后一行与第一行互换，然后重新排序得

$$\sigma^{-1}=\begin{bmatrix}3&1&5&4&6&2\\1&2&3&4&5&6\end{bmatrix}=\begin{bmatrix}1&2&3&4&5&6\\2&6&1&4&3&5\end{bmatrix}.$$

$$\begin{array}{cccccccc}
 & 1 & 2 & 3 & 4 & 5 & 6\\
\sigma & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
 & 3 & 1 & 5 & 4 & 6 & 2\\
\tau & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
 & 1 & 5 & 2 & 6 & 4 & 3
\end{array}
\qquad
\begin{array}{cccccccc}
 & 1 & 2 & 3 & 4 & 5 & 6\\
\tau & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
 & 5 & 3 & 1 & 6 & 2 & 4\\
\sigma & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
 & 6 & 5 & 3 & 2 & 1 & 4
\end{array}
\qquad
\begin{array}{cccccccc}
 & 1 & 2 & 3 & 4 & 5 & 6\\
\sigma & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
 & 3 & 1 & 5 & 4 & 6 & 2\\
\sigma & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
 & 5 & 3 & 6 & 4 & 2 & 1
\end{array}$$

(a)　　(b)　　(c)

图 12－8

12.13 设 S 是平面 $\mathbf{R}^2$ 上的正方形，如图 12－9. 它的中心在原点 O. S 的四个顶点逆时针标上 1 到 4.（a）定义 S 的对称群 G.（b）列出 G 的元素.（c）求 G 的最小生成集.

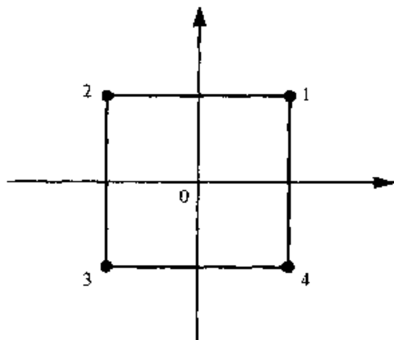


图 12－9

解☞ (a) S 的一个对称变换 σ 是一严格的 S 与它本身之间的 1－1 对应.（这里严格意思是点与点之间的距离不变），S 的对称群 G 是 S 的所有对称变换在映射的复合下构成的群.

(b) 共有八个对称变换. 对于 $\alpha=0°,90°,180°$ 和 $270°$，设 $\sigma(\alpha)$ 是 S 绕中心旋转 α 度所得的对称变换，设 $\tau(\alpha)$ 是 S 关于 y 轴的反射绕中心旋转 α 度所得. 任何 S 的对称变换 σ 都是由 S 的顶点决定，因此 σ 可以表示为 S_4 的一个置换，于是

$$\sigma(0°)=\begin{bmatrix}1&2&3&4\\1&2&3&4\end{bmatrix},\quad \sigma(90°)=\begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix},$$

$$\sigma(180°)=\begin{bmatrix}1&2&3&4\\3&4&1&2\end{bmatrix},\quad \sigma(270°)=\begin{bmatrix}1&2&3&4\\4&1&2&3\end{bmatrix},$$

$$\tau(0°)=\begin{bmatrix}1&2&3&4\\2&1&4&3\end{bmatrix},\quad \tau(90°)=\begin{bmatrix}1&2&3&4\\3&2&1&4\end{bmatrix},$$

$$\tau(180°)=\begin{bmatrix}1&2&3&4\\4&3&2&1\end{bmatrix},\quad \tau(270°)=\begin{bmatrix}1&2&3&4\\1&4&3&2\end{bmatrix}.$$

(c) 设 $a=\sigma(90°)$，$b=\tau(0°)$. 那么 a 和 b 就形成了 G 的生成元的最小集. 特别地，

$$\sigma(0°)=a^4,\ \sigma(90°)=a,\ \sigma(180°)=a^2,\ \sigma(270°)=a^3,$$
$$\tau(0°)=b,\ \tau(90°)=ba,\ \tau(180°)=ba^2,\ \tau(270°)=ba^3.$$

G 不是循环群，因此不是由一个元素生成的.（可以证明 $a^4=e,b^2=e$ 和 $bab=a^{-1}$ 完整地刻画了 G.）

12.14 设 H 和 K 是群，(a) 定义 H 和 K 的直积 $G=H\times K$. (b) $G=H\times K$ 的单位元和阶是什么？(c) 描述并求出群 $G=\mathbf{Z}_2\times\mathbf{Z}_2$ 的乘法表.

解 ☞ (a) 设 $G=H\times K$.

$$(h,k)*(h'k')=(hh',kk').$$

那么 G 是个群(问题 12.73)，称为 H 和 K 的直积.

(b) 元素 $e=(e_H,e_K)$ 是 G 的单位元且 $|G|=|H||K|$.

(c) 由于 $\mathbf{Z}_2$ 有两个元素，故 G 有四个元素，设

$$e=(0,0),\ a=(1,0),\ b=(0,1),\ c=(1,1).$$

G 的乘法表见图 12-10，注意 G 是阿贝尔群，因为这个表是对称的，并且

$$a^2=e,\quad b^2=e,\quad c^2=e.$$

于是 G 不是循环群. 因此 $G\not\cong\mathbf{Z}_4$.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

图 12-10

12.15 设 G 是一个群，A 为一非空集合.

(a) 定义“G 作用于 A”

(b) 定义 $a\in A$ 的稳定因子 Ha.

(c) 证明 Ha 是 G 的一个子群.

解 ☞ (a) 设 PERM(A)表示 A 的所有置换构成的群. 设 $\Psi:G\to\mathrm{PERM}(A)$ 是任一同态. 那么 G 称为作用于 A，其中 G 中每一个元素 g 都定义了一个置换 $g:A\to A$，由

$$g(a)=(\Psi(g))(a).$$

(习惯上，置换 $g:A\to A$ 直接给出，因此同态 Ψ 是隐出的定义).

(b) $a\in A$ 的稳定因子 Ha 是由 G 中所有作用在元素 a 上的变换构成，即

$$Ha=\{g\in G: g(a)=a\}.$$

(c) 因为 $e(a)=a$，我们得 $e\in Ha$. 设 $g,g'\in Ha$，那么 $(gg')(a)=g(g'(a))=g(a)=a$. 因此 $gg'\in Ha$，又因为 $g(a)=a$，故 $g^{-1}(a)=a$. 因此 $g^{-1}\in Ha$，这样，Ha 就是 G 的一个子群.

12.16 设 $S=\mathbf{R}^2$ 是笛卡儿坐标平面. 求 S 中 $a=(1,0)$ 的稳定因子，设作用在 S 上的群 G 为：

(a) $G=\mathbf{Z}\times\mathbf{Z}$ 且 G 作用在 S 上

$$g(x,y)=(x+m,y+n)，其中\ g=(m,n).$$

即 G 中每一个元素 g 都是 S 的一个平移.

(b) $G=(\mathbf{R},+)$ 且 G 作用在 S 上

$$g(x,y)=(x\cos g-y\sin g,x\sin g+y\cos g).$$

即 G 的每一个元素 g 都是 S 绕原点旋转角度 g.

解 ☞ (a) 设 $g=(m,n)$，那么

$$g(a)=g(1,0)=(1+m,n)=(1,0)=a.$$

当且仅当 $g=(0,0)$，因此 Ha 仅为 G 的单位元(0,0)

(b) 在任何旋转 2π 的倍数的变换下 a 不变，因此 $Ha=\{2\pi r: r\in\mathbf{Z}\}$.

12.17 证明定理 12.6：设 H 是群 G 的一个子群，那么右陪集 Ha 构成 G 的一个划分.

证明 ☞ 因为 $e\in H$，所以 $a=ea\in Ha$：即每一个元素都属于一个陪集. 事实上 $a\in Ha$. 现设 Ha 和 Hb 相交，设 $c\in Ha\cap Hb$，若能证明 $Ha=Hb$，则证明完成.

由于 c 既属于 Ha，又属于 Hb，我们有 $c=h_1a$，$c=h_2b$，其中 $h_1,h_2\in H$. 那么 $h_1a=h_2b$，故 $a=h_1^{-1}h_2b$. 设 $x\in Ha$，那么

$$x=h_3a=h_3h_1^{-1}h_2b.$$

其中 $h_3\in H$. 因为 H 是一子群，$h_3h_1^{-1}h_2\in H$，所以 $x\in Hb$. 因为 x 是 Ha 的任意元素，我们就有 $Ha\subseteq Hb$，类似地，$Hb\subseteq Ha$. 所以 $Ha=Hb$，定理得证.

12.18 设 H 是 G 的一个有限子群. 证明 H 和任何陪集 Ha 有同样多的元素.

证明 ☞ 设 $H=\{h_1,h_2,\cdots,h_n\}$，其中 H 有 n 个元素，那么 $Ha=\{h_1a,h_2a,\cdots,h_na\}$. 但是 $h_ia=$

$h_i a$ 蕴含 $h_i = h_j$，因此 Ha 中列出的 n 个元素是不同的，故 H 和 Ha 有相同数目的元素.

12.19 证明定理 12.7(拉格朗日定理) 设 H 是群 G 的一个有限子群，那么 H 的阶整除 G 的阶.

证明 ☞ 假设 H 有 r 个元素且有 s 个右陪集，如

$$H_{a_1}, H_{a_2}, \cdots, H_{a_s}.$$

由定理 12.6，陪集为 G 的划分和问题 12.18，每个陪集都有 r 个元素，因此 G 有 rs 个元素，所以 H 的阶整除 G 的阶.

12.20 设 G 是一阶数为 p 的群，其中 p 是素数，求 G 的所有子群.

证明 ☞ 由拉格朗日定理，G 的子群 H 的阶整除 G 的阶，故 $|H|=1$ 或 p，所以 $\{e\}$ 和 G 本身是 G 仅有的子群.

12.21 设 G 是一阶数为 n 的有限群. 证明对于任何元素 $a \in G$，有 $a^n = e$.

证明 ☞ 假设 m 是 a 的阶，那么 $a^m = e$. 由拉格朗日定理 m 整除 n. 不妨设 $n = mr$，那么

$$a^n = a^{mr} = (a^m)^r = e^r = e.$$

12.22 证明：循环群 G 的每一个子群都是循环的.

证明 ☞ 由于 G 是循环的，所以存在 $a \in G$，使得 $G = gp(a)$. 设 H 是 G 的一个子群. 如果 $H = \{e\}$，那么 $H = gp(e)$，故循环. 否则，H 包含 a 的非零次幂，由于 H 是一子群，它在逆元下一定封闭，故包含 a 的正次幂. 设 m 是使得 $a^m \in H$ 的最小次幂，我们说 $b = a^m$ 生成了 H. 设 x 为 H 中的任意其他元素，由于 $x \in G$，有 $x = a^n$，对于某个整数 n. n 被 m 除得商 q 和余数 r，即

$$n = mq + r.$$

其中 $0 \leqslant r < m$，那么

$$a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r,$$

故 $a^r = b^{-q} a^n$.

但 $a^n, b \in H$；由于 H 是一子群，$b^{-q} a^n \in H$，这就意味着 $a^r \in H$. 但是 m 是属于 H 的最小正整数次幂，因此 $r = 0$，故 $a^n = b^q$，这样 b 生成了 H，H 是循环的.

12.23 设 H 是一子群，现设 K 是群 G 的正规子群. 证明 HK 是一个 G 的子群.

证明 ☞ 我们必须证明 $e \in HK$ 和 HK 在乘法和逆元下封闭. 因为 H 和 K 是子群，$e \in H$，$e \in K$，故 $e = e \cdot e \in HK$. 假设 $x, y \in HK$，那么 $x = h_1 k_1$，$y = h_2 k_2$ 其中 $h_1, h_2 \in H$，$k_1, k_2 \in K$，那么

$$xy = h_1 k_1 h_2 k_2 = h_1 h_2 (h_2^{-1} k_1 h_2) k_2.$$

因为 K 是正规的，$h_2^{-1} k_1 h_2 \in K$. 又因为 H 和 K 是子群，$h_1 h_2 \in H$，$(h_2^{-1} k_1 h_2) k_2 \in K$，这样 $xy \in HK$. 故 HK 在乘法下封闭. 我们还有

$$x^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} = h_1^{-1} (h_1 k_1^{-1} h_1^{-1}).$$

由于 K 是一正规子群 $h_1 k_1^{-1} h_1^{-1} \in K$，而且 $h_1^{-1} \in H$. 因此 $x^{-1} \in HK$，从而 HK 在逆元下封闭，故 HK 是一个子群.

12.24 证明定理 12.8：设 H 是群 G 的一个正规子群，那么 G 中 H 的陪集在由 $(aH)(bH) = abH$ 定义的陪集乘法下形成一个群.

证明 ☞ 陪集的乘法的定义是有意义的，因为

$$(aH)(bH) = a(Hb)H = a(bH)H = ab(HH) = abH.$$

(这里我们用到了 H 是一正规子群，$Hb = bH$ 并由定理 12.61，$H \cdot H = H$)陪集的乘法结合律可由 G 满足乘法结合律得到. H 是 G/H 的单位元，因为

$$(aH)H = a(HH) = aH \quad \text{且} \quad H(aH) = (Ha)H = (aH)H = aH.$$

最后，$a^{-1}H$ 是 aH 的逆元，因为

$$(a^{-1}H)(aH) = a^{-1}aH = eH = H \quad \text{且}$$
$$(aH)(a^{-1}H) = aa^{-1}H = eH = H.$$

因此 G/H 在陪集乘法下构成群.

12.25 假设 $f: G \to G'$ 是一个群同态. 证明：(a) $f(e) = e'$；(b) $f(a^{-1}) = f(a)^{-1}$.

证明 ☞ (a) 由于 $e=ee$ 且 f 是同态，有

$$f(e)=f(ee)=f(e)f(e).$$

在上式两边同乘 $f(e)^{-1}$ 得到我们的结论.

(b) 由(a)部分和 $aa^{-1}=a^{-1}a=e$，有

$$e'=f(e)=f(aa^{-1})=f(a)f(a^{-1}) \quad 且$$
$$e'=f(e)=f(a^{-1}a)=f(a^{-1})f(a).$$

因此 $f(a^{-1})$ 是 $f(a)$ 的逆元，即 $f(a^{-1})=f(a)^{-1}$.

12.26 证明定理 12.9：设 $f:G\to G'$ 是一核为 K 的同态，那么 K 是 G 的正规子群，且 G/K 同构于 f 的像(与问题 12.8 比较，半群有类似的定理.)

证明 ☞ 证明 K 是正规的 由问题 12.19，$f(e)=e'$，因此 $e\in K$. 现设 $a,b\in K$ 且 $g\in G$，那么 $f(a)=e'$ 且 $f(b)=e'$. 因此

$$f(ab)=f(a)f(b)=e'e'=e'.$$
$$f(a^{-1})=f(a)^{-1}=e'^{-1}=e'.$$
$$f(gag^{-1})=f(g)f(a)f(g^{-1})=f(g)e'f(g)^{-1}=e'.$$

因此 ab,a^{-1} 和 $gag^{-1}\in K$，故 K 是一正规子群.

证明 $G/K\simeq H$，其中 H 是 f 的像 设 $\phi:G/K\to H$ 定义为

$$\phi(Ka)=f(a).$$

我们证明 ϕ 的定义是有意义的，即如果 $Ka=Kb$，那么 $\phi(Ka)=\phi(Kb)$. 假设 $Ka=Kb$，那么 $ab^{-1}\in K$ (问题 12.61)，那么 $f(ab^{-1})=e'$ 因此

$$f(a)f(b)^{-1}=f(a)f(b^{-1})=f(ab^{-1})=e'.$$

因此 $f(a)=f(b)$，且 $\phi(Ka)=\phi(Kb)$. 故 ϕ 是良好定义的，我们下一步证明 ϕ 是一同态

$$\phi(KaKb)=\phi(Kab)=f(ab)=f(a)f(b)=\phi(Ka)\phi(Kb).$$

因此 ϕ 是一同态. 下一步证明 ϕ 是 1-1 的，假设 $\phi(Ka)=\phi(Kb)$，那么

$$f(a)=f(b) \quad 或 \quad f(a)f(b)^{-1}=e' \quad 或$$
$$f(a)f(b^{-1})=e' \quad 或 \quad f(ab^{-1})=e'.$$

故 $ab^{-1}\in K$，且由问题 12.61 有 $Ka=Kb$. 这样 ϕ 是 1-1 的. 以下证明 ϕ 是映上的. 设 $h\in H$. 由于 H 是 f 的像，存在 $a\in G$ 使得 $f(a)=h$. 这样 $\phi(Ka)=f(a)=h$，因此 ϕ 是映上的. 所以 $G/K\cong H$，定理得证.

12.27 设 G 是一个群，$g\in G$. 定义函数 $\hat{g}:G\to G$ 为 $\hat{g}(x)=gxg^{-1}$，证明 $\hat{g}$ 是 G 到 G 的同构，即证明 (a) $\hat{g}$ 是一同态，(b) $\hat{g}$ 是 1-1 的，(c) $\hat{g}$ 是映上的.

证明 ☞ (a) 我们有 $\hat{g}(xy)=gxyg^{-1}=(gxg^{-1})(gyg^{-1})=\hat{g}(x)\hat{g}(y)$，因此 $\hat{g}$ 是一同态.

(b) 假设 $\hat{g}(x)=\hat{g}(y)$，那么 $gxg^{-1}=gyg^{-1}$，由消去律，$x=y$，故 $\hat{g}$ 是 1-1 的.

(c) 假设 $z\in G$，那么 $\hat{g}(g^{-1}zg)=gg^{-1}zgg^{-1}=z$. 因此 $\hat{g}$ 是映上的.

环，整环和域

12.28 考虑模 10 整数环 $\mathbf{Z}_{10}=\{0,1,2,\cdots,9\}$

(a) 求 $\mathbf{Z}_{10}$ 的单位.

(b) 求 -3，-8 和 3^{-1}.

(c) 设 $f(x)=2x^2+4x+4$. 求 $\mathbf{Z}_{10}$ 上 $f(x)$ 的根.

解 ☞ (a) 由问题 12.63 知，那些与模 10 互素的整数是 $\mathbf{Z}_{10}$ 中的单位. 因此单位是 1，3，7，9.

(b) 在环 R 中定义元素 $-a$，即为使得 $a+(-a)=(-a)+a=0$ 的元素，因此由 $\mathbf{Z}_{10}$ 中 $3+7=7+3=0$ 得 $-3=7$，类似地，$-8=2$. 在环中我们定义元素 a^{-1} 为使得 $a\cdot a^{-1}=a^{-1}\cdot a=1$ 的元素，因此 $3^{-1}=7$，由于 $\mathbf{Z}_{10}$ 中 $3\cdot 7=7\cdot 3=1$.

(c) 将 $\mathbf{Z}_{10}$ 中的 10 个元素都代入 $f(x)$ 中，看哪些结果为零，得

$$f(0)=4,\ f(2)=0,\ f(4)=2,\ f(6)=0,\ f(8)=4,$$
$$f(1)=0,\ f(3)=4,\ f(5)=4,\ f(7)=0,\ f(9)=2.$$

根就为 1，2，6，7. (本例表明 n 次多项式在一个环上可以有多于 n 个的根，但在域上不成立.)

12.29 证明在环 R 内：(i) $a\cdot 0=0\cdot a=0$；(ii) $a(-b)=-(a)b=-ab$；(iii) $(-1)a=-a$（当 R 有单位元 1 时）.

证明 ☞ (i) 因为 $0=0+0$，有

$$a\cdot 0=a(0+0)=a\cdot 0+a\cdot 0.$$

在上式两边加上 $-(a\cdot 0)$，得 $0=a\cdot 0$. 类似地 $0\cdot a=0$.

(ii) 用 $b+(-b)=(-b)+b=0$，有

$$ab+a(-b)=a(b+(-b))=a\cdot 0=0.$$
$$a(-b)+ab=a((-b)+b)=a\cdot 0=0.$$

因此 $a(-b)$ 是 ab 的相反数. 即 $a(-b)=-ab$. 类似地，$(-a)b=-ab$.

(iii) 有

$$a+(-1)a=1\cdot a+(-1)a=(1+(-1))a=0\cdot a=0,$$
$$(-1)a+a=(-1)a+1\cdot a=((-1)+1)a=0\cdot a=0.$$

因此 $(-1)a$ 是 a 的负元，即 $(-1)a=-a$.

12.30 在整环 D 中，证明：如果 $ab=ac$ 且 $a\neq 0$，那么 $b=c$.

证明 ☞ 由于 $ab=ac$，有

$$ab-ac=0,\ a(b-c)=0.$$

因为 $a\neq 0$，我们得 $b-c=0$，因为 D 没有零因子. 故 $b=c$.

12.31 假设 J 和 K 是环 R 的理想，证明 $J\cap K$ 是 R 的一个理想.

证明 ☞ 因为 J 和 K 是理想，$0\in J$ 且 $0\in K$，因此 $0\in J\cap K$. 现设 $a,b\in J\cap K$ 且设 $r\in R$，那么 $a,b\in J$ 且 $a,b\in K$. 因为 J 和 K 是理想，

$$a-b,ra,ar\in J\quad 且\quad a-b,ra,ar\in K.$$

因此 $a-b,ra,ar\in J\cap K$，故 $J\cap K$ 是一个理想.

12.32 设 J 是单位元为 1 的环 R 的一个理想. 证明：(a) 如果 $1\in J$，那么 $J=R$. (b) 如果任何单位 $u\in J$，那么 $J=R$.

证明 ☞ (a) 如果 $1\in J$，那么对于任何 $r\in R$，我们有 $r\cdot 1\in J$ 或 $r\in J$，因此 $J=R$.

(b) 如果 $u\in J$，那么 $u^{-1}u\in J$ 或 $1\in J$，因此由(a)得 $J=R$.

12.33 证明：(a) 有限的整环 D 是一个域.

(b) $\mathbf{Z}_p$ 是一个域，其中 p 是素数.

(c)（费马定理）如果 p 是素数，那么对于任意整数 a 有 $a^p\equiv a(\bmod p)$.

证明 ☞ (a) 假设 D 有 n 个元素，不妨设 $D=\{a_1,a_2,a_3,\cdots,a_n\}$，设 a 是 D 的任一非零元素. 考虑这 n 个元素

$$aa_1,aa_2,\cdots,aa_n.$$

因为 $a\neq 0$，有 $aa_i=aa_j$ 蕴含 $a_i=a_j$（问题 12.30）. 故上面 n 个元素是不同的，它们是 D 中元素的重排. 其中的一个不妨设 aa_k 等于 D 的单位元即 $aa_k=1$. 这样 a_k 就是 a 的逆元. 因为 a 是 D 的任意非零元，故我们说 D 是一个域.

(b) 回顾 $\mathbf{Z}_p=\{0,1,2,\cdots,p-1\}$. 我们证明 $\mathbf{Z}_p$ 没有零因子. 假设 $a*b=0$ 即在 $\mathbf{Z}_p$ 中 $ab\equiv 0(\bmod p)$，那么 p 整除 ab. 因为 p 是一个素数，p 整除 a 或 b. 即 $a\equiv 0(\bmod p)$ 或 $b\equiv 0(\bmod p)$，即在 $\mathbf{Z}_p$ 中 $a=0$ 或 $b=0$，因此 $\mathbf{Z}_p$ 没有零因子，故 $\mathbf{Z}_p$ 是一个整环. 由(a)得 $\mathbf{Z}_p$ 是一个域.

(c) 如果 p 整除 a，那么 $a\equiv 0(\bmod p)$. 故 $a^p\equiv a\equiv 0(\bmod p)$. 假设 p 不整除 a，那么 a 可以看做是 $\mathbf{Z}_p$ 的一个非零元. 由于 $\mathbf{Z}_p$ 是一个域，它的非零元在乘法下形成了阶为 $p-1$ 的群. 由问题 12.21，$a^{p-1}=1$ 在 $\mathbf{Z}_p$ 中. 换句话说，$a^{p-1}\equiv 1(\bmod p)$. 在两边同乘上 a 得 $a^p\equiv a(\bmod p)$，定理得证.

域上的多项式

12.34 设 $f(t)=t^3-2t^2-6t-3$. 已知 $f(t)$ 有一整数根，求 $f(t)$ 的根.

解 ☞ $f(t)$ 的整数根必在 $\pm 1,\pm 3$ 中，注意 $f(-1)=0$. 用综合除法或被 $t+1$ 除，得

$$\begin{array}{r|l} -1 & 1-2-6-3 \\ & \quad -1+3+3 \\ \hline & 1-3-3+0 \end{array}$$

因此 $t=-1$ 是一个根，$f(t)=(t+1)(t^2-3t-3)$. 我们可以对 t^2-3t-3 用求根公式得 $f(t)$ 的三个根

$$t=-1,\ t=(3+\sqrt{21})/2,\ t=(3-\sqrt{21})/2.$$

12.35 假设 $f(t)=2t^3-3t^2-6t-2$. 已知 $f(t)$ 有一有理根，求 $f(t)$ 的所有根.

解 ☞ $f(t)$ 的有理根必在 $\pm1,\pm2,\pm\frac{1}{2}$ 中，检验每一个可能的根，通过综合除法（或被 $2t+1$ 除）得，

$$\begin{array}{r|l} -\frac{1}{2} & 2-3-6-2 \\ & \quad -1+2+2 \\ \hline & 2-4-4+0 \end{array}$$

因此 $t=-\frac{1}{2}$ 是一个根，且

$$f(t)=\left(t+\frac{1}{2}\right)(2t^2-4t-4)=(2t+1)(t^2-2t-2).$$

现在对 t^2-2t-2 用求根公式得 $f(t)$ 的三个根

$$t=-\frac{1}{2},\ t=1+\sqrt{3},\ t=1-\sqrt{3}.$$

12.36 设 $f(t)=t^4-3t^3+3t^2+3t-20$，已知 $1+2\mathrm{i}$ 是一个根，求 $f(t)$ 的所有根.

解 ☞ 因为 $1+2\mathrm{i}$ 是一个根，故 $1-2\mathrm{i}$ 也是一个根，且 $c(t)=t^2-2t+5$ 是 $f(t)$ 的一个因式. $f(t)$ 被 $c(t)$ 除得

$$f(t)=(t^2-2t+5)(t^2-t-4).$$

对 t^2-t-4 用求根公式得出 $f(t)$ 的另外两个根. 即 $f(t)$ 的 4 个根如下

$$t=1+2\mathrm{i},\ t=1-2\mathrm{i},\ t=(1+\sqrt{17})/2,\ t=(1-\sqrt{17})/2.$$

12.37 设 $K=\mathbf{Z}_8$，求出 $f(t)=t^2+6t$ 的所有根.

解 ☞ 这里 $\mathbf{Z}_8=\{0,1,2,\cdots,7\}$，将 $\mathbf{Z}_8$ 中每一个元素都代入 $f(t)$ 得

$$f(0)=0,\ f(2)=0,\ f(4)=0,\ f(6)=0.$$

那么 $f(t)$ 有 4 个根，$t=0,2,4,6$.（因为 K 不是域，故定理 12.21 不满足.）

12.38 假设 $f(t)$ 是一个次数为奇数 n 的实多项式.

(a) 用代数方法证明 $f(t)$ 有一个实根.

(b) 用几何方法证明 $f(t)$ 有一个实根.

证明 ☞ (a) $f(t)$ 的复根总是成对出现的. 因为 $f(t)$ 有奇数个根，故 $f(t)$ 必至少有一个实根.

(b) 假设 $f(t)$ 的首项系数是正的［否则，将 (-1) 乘上 $f(t)$］. 因为 $\deg(f)=n$，其中 n 是奇数，有

$$\lim_{t\to+\infty}f(t)=+\infty,\ \lim_{t\to-\infty}f(t)=-\infty.$$

因此 $f(t)$ 的图像与 t 轴至少有一个交点，见图 12-11.

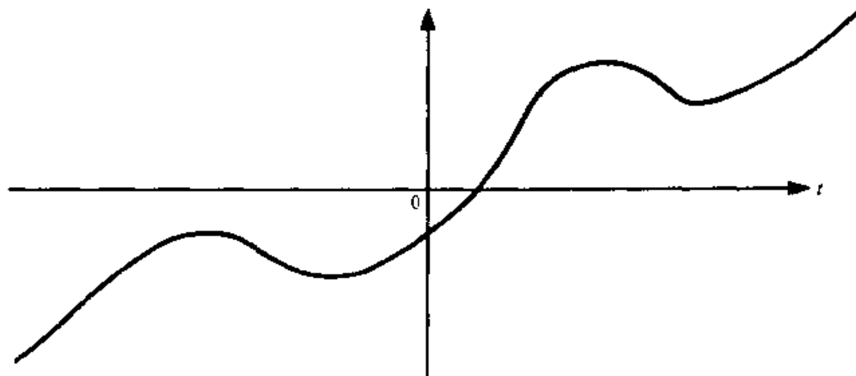


图 12-11

12.39 证明定理 12.15(带余除法) 设 $f(t)$和 $g(t)$是域 K 上的多项式且$g(t)\neq 0$,那么存在多项式 $q(t)$和 $r(t)$,使得

$$f(t)=q(t)g(t)+r(t).$$

其中或者 $r(t)\equiv 0$ 或 $\deg(r)<\deg(g)$.

证明 ☞ 如果 $f(t)=0$ 或 $\deg(f)<\deg(g)$.那么有要求的表达式$f(t)=0g(t)+f(t)$. 现设$\deg(f)\geqslant\deg(g)$,不妨设 $f(t)=a_nt^n+\cdots+a_1t+a_0$,$g(t)=b_mt^m+\cdots+b_1t+b_0$,其中 $a_n,b_m\neq 0$ 且 $n\geqslant m$. 于是有多项式

$$f_1(t)=f(t)-\frac{a_n}{b_m}t^{n-m}g(t). \tag{1}$$

(这是"长除法"的第一步.)那么 $\deg(f_1)<\deg(f)$. 由归纳法存在多项式 $q_1(t)$和 $r(t)$,使得 $f_1(t)=q_1(t)g(t)+r(t)$,其中 $r(t)\equiv 0$ 或 $\deg(r)<\deg(g)$. 将它代入(1)得

$$f(t)=\left(q_1(t)+\frac{a_n}{b_m}t^{n-m}\right)g(t)+r(t).$$

这就是所要求的表达式.

12.40 证明定理 12.18:假设 $f(t)$是域 K 上的一个多项式,$\deg(f)=n$,那么 $f(t)$至多有 n 个根.

证明 ☞ 对 n 用归纳法. 如果 $n=1$,那么 $f(t)=at+b$,$f(t)$有惟一的根 $t=-b/a$. 假设$n>1$,如果$f(t)$没有根,那么定理是正确的,假设 $a\in K$ 是 $f(t)$的一个根,那么

$$f(t)=(t-a)g(t). \tag{1}$$

其中 $\deg(g)=n-1$. 我们说 $f(t)$的任意其他根必也是 $g(t)$的一个根. 假设$b\neq a$是 $f(t)$的另一根. 将$t=b$代入(1)得 $0=f(b)=(b-a)g(b)$. 因为 K 没有零因子且 $b-a\neq 0$,必有 $g(b)=0$. 由归纳法,$g(t)$至多有 $n-1$ 个根. 因此 $f(t)$至多有 $n-1$ 个不同于 a 的根. 因此 $f(t)$至多有 n 个根.

12.41 证明定理 12.19:假设一个有理数 p/q(最简形式)是多项式

$$f(t)=a_nt^n+\cdots+a_1t+a_0$$

的一个根,其中所有的系数 $a_n,\cdots,a_1,a_0$ 是整数. 那么 p 整除 a_0,q 整除首项系数 a_n. 特别地如果 $c=p/q$ 是一整数,那么 c 整除 a_0.

证明 ☞ 将 $t=p/q$ 代入 $f(t)=0$ 得 $a_n(p/q)^n+\cdots+a_1(p/q)+a_0=0$. 在两边同乘 q^n 得

$$a_np^n+a_{n-1}p^{n-1}q+a_{n-2}p^{n-2}q^2+\cdots+a_1pq^{n-1}+a_0q^n=0 \tag{1}$$

因为 p 整除(1)的前 n 项,故 p 一定整除 a_0q^n. 已知 p 和 q 互素,故 p 整除 a_0,类似地,q 整除(1)的后 n 项,因此 q 整除首项 a_np^n. 因为 p 和 q 互素,q 整除 a_n.

12.42 证明定理 12.20:域 K 上的多项式环 $K[t]$是一个主理想整环(PID). 如果 J 是$K[t]$中的一个理想,那么惟一标准多项式 d 生成 J,即 J 中每一个多项式 f 是 d 的倍数.

证明 ☞ 设 d 是 J 中次数最低的一个多项式. 因为我们可以在 d 上乘上一个非零数使得它仍在 J 中,可以假设 d 是一个标准多项式. 现设 $f\in J$,由带余除法,存在 q 和 r 使得 $f=qd+r$,其中或者 $r=0$或 $\deg(r)<\deg(d)$. 现在 $f,d\in J$ 蕴含着 $qd\in J$,因此 $r=f-qd\in J$. 但是 d 是 J 中次数最小的多项式,于是 $r=0$,$f=qd$ 即 d 整除 f. 还须证明 d 是惟一的,如果 d'是生成 J 的另一个标准多项式,那么 d 整除 d'且 d'整除 d. 这就推出 $d=d'$,因为 d 和 d'都是标准形式,故定理得证.

12.43 证明定理 12.21:设 f 和 g 是 $K[t]$的多项式. 那么存在惟一的标准多项式 d 使得(i) d 整除 f 和 g. (ii) 如果 d'整除 f 和 g,那么 d'整除 d.

证明 ☞ 集合 $I=\{mf+ng:m,n\in K[t]\}$是一个理想. 设 d 是生成 I 的标准多项式. $f,g\in I$,故 d 整除 f 和 g. 现设 d'整除 f 和 g,J 是 d'生成的理想,那么$f,g\in J$,因此 $I\subseteq J$. 于是,$d\in J$,故 d' 整除 d. 还需要证明 d 是惟一的. 如果 d_1 是另一个 f 和 g 的标准的最大公因式,那么 d 整除 d_1 且 d_1 整除 d,这就意味着 $d=d_1$,因为 d 和 d_1 是标准的. 因此定理得证.

12.44 证明推论 12.22:设 d 是 f 和 g 的最大公因式,那么存在多项式 m 和 n 使得 $d=mf+ng$. 特别地,如果 f 和 g 互素,那么存在多项式 m 和 n 使得 $mf+ng=1$.

证明 ☞ 由问题 12.43 中定理 12.21 的证明得,最大公因式 d 生成理想 $I=\{mf+ng:m,n\in K$

$[t]\}$，因此存在多项式 m 和 n 使得 $d=mf+ng$.

12.45 证明引理 12.23：假设 $p\in K[t]$ 不可约. 如果 p 整除多项式的积 $f\cdot g$，$f,g\in K[t]$，那么 p 整除 f 或 p 整除 g. 更一般地，如果 p 整除 n 个多项式的积 $f_1\cdot f_2\cdots f_n$，那么 p 整除它们当中的一个.

证明 ☞ 假设 p 整除 $f\cdot g$，但不整除 f. 因为 p 不可约，f 和 p 必互素. 那么存在多项式 $m,n\in K[t]$，使得 $mf+np=1$. 在方程上乘 g，我们得到 $mfg+npg=g$. 但 p 整除 fg，故 p 整除 mfg，且 p 整除 npg，因此 p 整除和 $g=mfg+npg$.

现设 p 整除 $f_1\cdot f_2\cdots f_n$. 如果 p 整除 f_1，那么命题得证. 如果不整除 f_1，那么由上面的结论，p 整除积 $f_2\cdots f_n$. 对 n 用归纳法，p 整除多项式 $f_2\cdots f_n$ 中的一个. 所以引理得证.

12.46 证明定理 12.24（惟一分解定理） 设 f 是 $K[t]$ 中一非零多项式，那么 f 除顺序外可惟一写成积 $f=kp_1p_2\cdots p_n$ 的形式，其中 $k\in K$ 且 p_i 是 $K[t]$ 中的标准不可约多项式.

证明 ☞ 首先证明积的存在性. 如果 f 不可约或 $f\in K$，那么积显然存在. 另外，假设 $f=g\cdot h$，其中 g 和 h 不是数量，那么 g 和 h 的次数小于 f 的次数. 由归纳法得，$g=k_1g_1g_2\cdots g_r$，$h=k_2h_1h_2\cdots h_s$ 其中 $k_1,k_2\in K$ 且 g_i 和 h_j 是标准不可约多项式. 于是 $f=(k_1k_2)g_1g_2\cdots g_rh_1h_2\cdots h_s$ 是我们要证的表达式.

下证这样的积 f 除顺序外的惟一性. 假设

$$f=kp_1p_2\cdots p_n=k'q_1q_2\cdots q_m\text{，其中 }k,k'\in K$$

且 $p_1,\cdots,p_n,q_1,\cdots q_m$ 是标准不可约多项式. 现在 p_1 整除 $k'q_1\cdots q_m$，因为 p_1 是不可约的. 由引理 12.23 它必须整除 q_i 中之一. 不妨设 p_1 整除 q_1，因为 p_1 和 q_1 都不可约且标准，$p_1=q_1$. 于是，$kp_2\cdots p_n=k'q_2\cdots q_m$. 由归纳法，有 $n=m$ 且 $p_2=q_2,\cdots,p_n=q_m$（q_i 经过重排），还可得 $k=k'$. 故定理得证.

12.47 证明定理 12.25：假设 $f(t)$ 是实数域 **R** 上的一个多项式，且复数 $z=a+bi$，$(b\neq 0)$ 是 $f(t)$ 的一个根. 那么共轭复数 $\bar{z}=a-bi$ 也是 $f(t)$ 的一个根，因此

$$c(t)=(t-z)(t-\bar{z})=t^2-2at+a^2+b^2$$

是 $f(t)$ 的一个因式.

证明 ☞ 因为 $\deg(c)=2$，故存在 $q(t)$ 和实数 M 和 N，使得

$$f(t)=c(t)q(t)+Mt+N \tag{1}$$

由于 $z=a+bi$ 是 $f(t)$ 和 $c(t)$ 的根，将 $t=a+bi$ 代入(1)，得

$$f(z)=c(z)q(z)+M(z)+N\quad\text{或}\quad 0=0q(z)+M(z)+N\quad\text{或}$$
$$M(a+bi)+N=0.$$

因此 $Ma+N=0$ 且 $Mb=0$. 因为 $b\neq 0$，我们有 $M=0$，那么 $0+N=0$ 或 $N=0$. 于是 $f(t)=c(t)q(t)$ 且 $\bar{z}=a-bi$ 是 $f(t)$ 的一个根.

补 充 题

运算和半群

12.48 设 $*$ 为实数集 **R** 上的运算，定义为 $a*b=a+b+2ab$.

(a) 求 $2*3$，$3*(-5)$ 和 $7*(1/2)$.

(b) $(\mathbf{R},*)$ 是半群吗？它可交换吗？

(c) 求单位元.

(d) 哪些元素有逆，是什么？

12.49 设 A 是由 $a*b=a$ 定义的运算下的一个非空集合，且已知 A 不只有一个元素.(a) A 是半群吗？(b) A 可交换吗？(c) A 有单位元吗？(d) 如果有，哪些元素有逆元，逆元是什么？

12.50 设 $A=\{a,b\}$，求 A 上运算的个数，并且写出一个既无结合律又无交换律的运算.

12.51 设 $A=\{\cdots,-9,-6,-3,0,3,6,9,\cdots\}$，即 3 的倍数. A 在(a) 加法 (b) 乘法 (c) 减法 (d) 除法(除 0 外)下封闭吗？

12.52 求一个含三个元素的集合 A 使得其在(a) 乘法(b) 加法下封闭.

12.53 设 S 是一无限集，A 是 S 的有限子集的集合，B 是 S 的无限子集的集合.

(a) A 在(i) 并 (ii) 交 (iii) 补下封闭吗?

(b) B 在(i) 并 (ii) 交 (iii) 补下封闭吗?

12.54 设 $S=\mathbf{Q}\times\mathbf{Q}$ 是定义了下面运算 * 的有序有理数偶的集合

$$(a,b)*(x,y)=(ax,ay+b).$$

(a) 求$(3,4)*(1,2)$和$(-1,3)*(5,2)$.

(b) S 是半群吗? 可交换吗?

(c) 求 S 的单位元.

(d) 如果有，哪些元素有逆元，逆元是什么?

12.55 设 $S=\mathbf{N}\times\mathbf{N}$ 是定义了下面运算 * 的有序正整数偶的集合

$$(a,b)*(c,d)=(ad+bc,bd)$$

(a) 求$(3,4)*(1,5)$和$(2,1)*(4,7)$.

(b) 证明 * 是可结合的(因此 S 是一个半群).

(c) 定义 $f:(S,*)\to(\mathbf{Q},+)$ 为 $f(a,b)=a/b$. 证明 f 是同态.

(d) 求 S 中由同态 f 决定的同余关系～.

(e) 描述 $S/\sim$. $S/\sim$ 有单位元吗? 它有逆元吗?

群

12.56 考虑在模 20 加法下的 $\mathbf{Z}_{20}=\{0,1,\cdots,19\}$，设 H 是由 5 生成的 $\mathbf{Z}_{20}$ 的子群.

(a) 求 H 的元素和阶. (b) 求 $\mathbf{Z}_{20}$ 中 H 的陪集.

12.57 考虑在模 18 乘法下的 $G=\{1,5,7,11,13,17\}$.

(a) 建立 G 的乘法表.

(b) 求 5^{-1}, 7^{-1}, 和 17^{-1}.

(c) 求由(i) 5 (ii) 13 生成的群和它们的阶.

(d) G 是循环群吗?

12.58 考虑在模 12 加法下的 $G=\{1,5,7,11\}$. (a)求每个元素的阶. (b)G 是循环群吗? (c)求出所有 G 的子群.

12.59 考虑对称群 S_4，设

$$\alpha=\begin{bmatrix}1&2&3&4\\3&4&2&1\end{bmatrix},\beta=\begin{bmatrix}1&2&3&4\\2&4&3&1\end{bmatrix}.$$

(a) 求 $\alpha\beta$, $\beta\alpha$, α^2 和 α^{-1}

(b) 求 α, β 和 $\alpha\beta$ 的阶.

12.60 证明群 G 上的下列结论.

(a) 单位元 e 是惟一的.

(b) G 中每一个元素都有逆元 a^{-1}.

(c) $(a^{-1})^{-1}=a$, $(ab)^{-1}=b^{-1}a^{-1}$. 更一般地，$(a_1a_2\cdots a_k)^{-1}=a_k^{-1}\cdots a_2^{-1}a_1^{-1}$.

(d) $ab=ac$ 可推出 $b=c$，且 $ba=ca$ 亦可推出 $b=c$.

(e) 对于任意整数 r 和 s，有 $a^ra^s=a^{r+s}$ 且 $(a^r)^s=a^{rs}$.

(f) G 是阿贝尔群当且仅当对于所有的 $a,b\in G$ 有 $(ab)^2=a^2b^2$ 成立.

12.61 设 H 是 G 的一个子群. 证明: (a)$H=Ha$ 当且仅当 $a\in H$. (b) $Ha=Hb$ 当且仅当 $ab^{-1}\in H$. (c) $HH=H$.

12.62 证明命题 12.5: 群 G 的子集是 G 的一个子群，如果(a)$e\in H$，且(b)对于所有的 $a,b\in H$，有 $ab,a^{-1}\in H$.

12.63 设 G 是一群.

(a) 证明 G 的任意个子群的交集是 G 的一个子群.

(b) 假设 A 是 G 的一个子集. 证明 $gp(A)$ 等于所有 G 中包含 A 的子群的交集.

(c) 证明 G 的任意个正规子群的交集是 G 的一个正规子群.

12.64 假设 G 是一阿贝尔群，证明任何商群 G/H 都是阿贝尔群.

12.65 假设 $|G|=p$，其中 p 是一素数. 证明(a)除$\{e\}$和 G 外 G 无其他子群. (b)G 是循环群且每一个元素 $a\neq$

e 生成 G.

12.66 证明 $G=\{1,-1,i,-i\}$ 是乘法下的一个群.利用同构映射 $f:G\to \mathbf{Z}_4$ 证明 $G\simeq \mathbf{Z}_4$.

12.67 设 H 是仅有两个右陪集的群 G 的一个子群.证明 H 是正规的.

12.68 设 S 是一正 n 边形,G 是 S 的对称群.(a)求 G 的阶.(b) 证明 G 是由满足 $a^n=e,b^2=e$ 且 $b^{-1}ab=a^{-1}$ 的两元素 a 和 b 生成的.(G 称为二面体群)

12.69 假设群 G 作用在集合 S 上,不妨设通过同态 $\Psi:G\to \mathrm{PERM}(S)$ 作用的.

(a) 证明对于任意的 $s\in S$(i) $e(s)=s$,且(ii) $(gg')(s)=g(g'(s))$,其中 $g,g'\in G$.

(b) 任何 $s\in S$ 的轨迹 G_s 定义为 $G_s=\{g(s):g\in G\}$,证明轨迹形成 S 的一个划分.

(c) 证明 $|G_s|=[G:H_s]$ 是 G 中 s 的稳定因子 H_s 的陪集的数目:(回顾 $H_s=\{g\in G:g(s)=s\}$.)

12.70 设 G 是一个阿贝尔群且设 n 是一正整数.证明由 $f(a)=a^n$ 定义的函数 $f:G\to G$ 是一个同态.

12.71 设 G 是满足 $|z|=1$ 的复数 z 形成的乘法群,$\mathbf{R}$ 是实数加法群.证明 $G\simeq \mathbf{R}/\mathbf{Z}$.

12.72 假设 H 和 N 是 G 的子群且 N 是正规的,证明(a) HN 是 G 的一个子群.(b) $H\cap N$ 是 H 的一个正规子群.(c) $H/(H\cap N)\simeq HN/N$.

12.73 设 H 和 K 是群,设 G 是在下列运算下的积集合 $H\times K$,

$$(h,k)*(h',k')=(hh',kk').$$

(a) 证明 G 是一个群(称为 H 和 K 的直积).

(b) 设 $H'=H\times\{e\}$.证明:(i) $H'\cong H$;(ii) H' 是一个 G 的正规子群.(iii) $G/H'\cong K$.

环

12.74 考虑整数模 12 的环 $\mathbf{Z}_{12}=\{0,1,\cdots,11\}$.

(a) 求 $\mathbf{Z}_{12}$ 的单位.

(b) 求在 $\mathbf{Z}_{12}$ 上 $f(x)=x^2+4x+4$ 的根.

(c) 求 $\mathbf{Z}$ 的陪伴元.

12.75 考虑整数模 30 的环 $\mathbf{Z}_{30}=\{0,1,\cdots,29\}$.

(a) 求 $-2,-7$ 和 -11.(b) 求 $7^{-1},11^{-1}$ 和 26^{-1}.

12.76 证明环 R 中:

(a) $(-a)(-b)=ab$;(b) $(-1)(-1)=1$,如果 R 有单位元 1.

12.77 假设对于每一个 $a\in R$ 有 $a^2=a$(这样的环称为布尔环).证明 R 是可交换的.

12.78 设 R 是有单位元 1 的一个环,我们将 R 转化为另一个环 R' 定义

$$a+b=a+b+1 \quad 且\ a*b=ab+a+b$$

(a) 证明 R' 是一个环.(b) 确定 R' 的 0 元素和 1 元素.

12.79 设 G 是任意(加法)阿贝尔群.定义 G 中的乘法,对于每一个 $a,b\in G$ 有 $a\cdot b=0$.证明这样将使 G 成为一个环.

12.80 设 J 和 K 是环 R 的理想.证明 $J+K$ 和 $J\cap K$ 也是 R 的理想.

12.81 设 R 是一个有单位元的环.证明 $(a)=\{ra:r\in R\}$ 是包含 a 的最小理想.

12.82 证明 R 和 $\{0\}$ 是任何环 R 的理想.

12.83 证明:(a) 环 R 的单位在乘法下形成群.

(b) $\mathbf{Z}_m$ 中的单位是那些和 m 互素的整数.

12.84 对于任意整数 m,证明 $m\mathbf{Z}=\{rm:r\in \mathbf{Z}\}$ 是一个环,并且证明 $2\mathbf{Z}$ 和 $3\mathbf{Z}$ 不同构.

12.85 证明定理 12.10:设 J 是环 R 的一个理想,那么陪集的集合 $\{a+J:a\in R\}$.在下面的运算下构成环

$$(a+J)+(b+J)=a+b+J,\ (a+J)(b+J)=ab+J.$$

12.86 证明定理 12.11:设 $f:R\to R'$ 是核为 K 的环同态,那么 K 是 R 中的一个理想且商群 R/K 同构于 $f(R)$.

12.87 设 J 是环 R 的一个理想,考虑正则映射 $f:R-R/J$,$f(a)=a+J$.证明:

(a) f 是一个环同态,(b) f 是一个满射.

12.88 假设 J 是环 R 中的一个理想,证明:

(a) 如果 R 可交换,那么 R/J 也可交换.

(b) 如果 R 有单位元 1 且 $1\notin J$,那么 $1+R$ 是 R/J 的单位元.

整环和域

12.89 证明整环 D 中,如果 $x^2=1$,那么 $x=0$ 或 $x=1$.

12.90 设 R 是一个无零因子的有限交换环,证明 R 是一个整环即 R 有单位元 1.

12.91 证明 $F=\{a+b\sqrt{2}; a,b$ 为有理数$\}$是一个域.

12.92 证明 $F=\{a+b\sqrt{2}; a,b$ 为整数$\}$是一个整环但不是域.

12.93 一个复数 $a+bi$(其中 a,b 是整数)称为高斯整数. 证明高斯整数集 G 是一个整环,并且证明单位为 $\pm1,\pm i$.

12.94 设 R 是一个整环并且 J 是 R 中的一个理想. 证明商环 R/J 是一个整环当且仅当 J 是一个素理想. (一个理想 J 称为素理想,如果 $ab\in J$ 可以推出 $a\in J$ 或 $b\in J$)

12.95 设 R 是单位元为 1 的交换环,J 是 R 中的一个理想. 证明商环 R/J 是一个域当且仅当 J 是一个极大理想(一个理想 J 称为极大理想,如果 $J\neq R$ 且没有理想 K 严格介于 J 和 R 之间,即如果 $J\subseteq K\subseteq R$,那么 $J=K$ 或 $K=R$).

12.96 设 D 是形如$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$的 2×2 实矩阵形的环,证明 D 同构于复数域 C,而 D 是一个域.

12.97 证明域 K 的理想只能为$\{0\}$或 K 本身.

12.98 设 $f:K\to K'$ 是域 K 到域 K' 的一个同态映射. 证明 f 是嵌入的. 即 f 是 1-1 的(我们假设 $f(1)\neq0$).

12.99 考虑整环 $D=\{a+b\sqrt{3}: a,b$ 是整数$\}$[见例 12.16(b)],如果 $\alpha=a+b\sqrt{13}$,我们定义 $N(\alpha)=a^2-18b^2$. 证明:(i)$N(\alpha\beta)=N(\alpha)N(\beta)$;(ii)$\alpha$ 是一个单位当且仅当 $N(\alpha)=\pm1$;(iii)D 的单位是 ±1, $18\pm5\sqrt{13}$ 和 $-18\pm5\sqrt{13}$;(iv)数 $2,3-\sqrt{13}$ 和 $-3-\sqrt{13}$ 是不可约的.

域上的多项式

12.100 求 $f(t)$ 的根,已知 $f(t)$ 有一个整数根:(a) $f(t)=t^3-t^2-11t-10$;(b) $f(t)=t^3+2t^2-13t-6$.

12.101 求 $f(t)$ 的根,已知 $f(t)$ 有一有理根:(a) $f(t)=2t^3-3t^2-16t-7$;(b) $f(t)=2t^3-t^2-9t-9$.

12.102 求 $f(t)=t^4+3t^3+8t^2-17t-13$ 的根,已知 $t=2+3i$ 是一个根.

12.103 求 $f(t)=t^4+3t^3-t^2-8t-10$ 的根,已知 $t=1-i$ 是一个根.

12.104 对于每一个数量 $a\in K$,定义赋值映射 $\Psi_a:K[t]\to K$ 为 $\Psi_a(f(t))=f(a)$. 证明 Ψ_a 是一个环同态.

12.105 证明命题 12.14.

12.106 证明定理 12.26.

补充题答案

12.48 (a) 17, −32, 29/2; (b) 是,是; (c) 零; (d) 如果 $a\neq1/2$,那么 a 有逆元 $-a/(1+2a)$.

12.49 (a) 是; (b) 不是; (c) 不是; (d) 当没有单位元时讨论逆元无意义.

12.50 16,因为对于 a,b 的乘积 aa,ab,ba 和 bb 都有两种选择. 图 12-12 中 $ab\neq ba$,而且,$(aa)b=bb=a$,但 $a(ab)=aa=b$.

*	a	b
a	b	a
b	b	a

图 12-12

12.51 (a) 是; (b) 是; (c) 是; (d) 不是.

12.52 (a) $\{-1,1,0\}$; (b) 没有集合.

12.53 (a) 是,是,不是; (b) 是,不是,不是.

12.54 (a) (3,10), (−5,1); (b) 是;不是; (c) (1,0); (d) 如果 $a\neq0$,元素(a,b)有一个逆元,它的逆元是 $(1/a,-b/a)$.

12.55 (a) (19,20), (18,7); (b) 是; (d) 如果 $ad=bc$ 则$(a,b)\sim(c,d)$; (e) $S/\sim$ 在加法下同构于正有理数

集，故 $S/\sim$ 没有单位元和逆元.

12.56 (a) $H=\{0,5,10,15\}$，$|H|=3$.

(b) $H, 1+H=\{1,6,11,16\}, 2+H=\{2,7,12,17\}, 3+H=\{3,8,13,18\}, 4+H=\{4,9,14,19\}$.

12.57 (a) 见图 12-13.

×	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

图 12-13

(b) $5^{-1}=11, 7^{-1}=13, 17^{-1}=17$.

(c) (i) $gp(5)=G, |5|=6$; (ii) $gp(13)=\{1,7,13\}, |13|=3$.

(d) 是，因为 $G=gp(5)$.

12.58 (a) $|1|=1, |5|=2, |7|=2, |11|=2$; (b) 不是; (c) $G, \{1\}, \{1,7\}, \{1,5\}, \{1,11\}$.

12.59 (a) $\alpha\beta=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 4 & 2\end{pmatrix}$，$\beta\alpha=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$.

$\alpha^2=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$，$\alpha^{-1}=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 1 & 2\end{pmatrix}$.

(b) $|\alpha|=4$，$|\beta|=3$，$|\alpha\beta|=4$.

12.66 $f(1)=0$; $f(i)=1$; $f(-1)=2$; $f(-i)=3$.

12.74 (a) 1,5,7,11; (b) 4,10; (c) $\{2,10\}$.

12.75 (a) $-2=28$，$-7=23$，$-11=19$.

(b) $7^{-1}=13$，$11^{-1}=11$，因为 26 不是一个单位，所以 26^{-1} 不存在.

12.77 应用 $a+a=(a+a)^2$ 证 $-a=a$，然后应用 $(a+b)^2=a+b$ 证 $ab=-ba$.

12.78 (b) -1 是零元素且 0 是 1 元素.

12.96 设 $f:D\to C$ 是 $\begin{bmatrix}a & -b\\ b & a\end{bmatrix}$ 到 $a+bi$ 的映射. 证明 f 是一同构.

12.98 提示：利用问题 12.97.

12.100 (a) $-2, (3\pm\sqrt{29})/2$; (b) $3, (-5\pm\sqrt{17})/2$.

12.101 (a) $-\frac{1}{2}, 1\pm 2\sqrt{2}$; (b) $\frac{3}{2}, (-1\pm\sqrt{13})/2$.

12.102 $2\pm 3i$; $(1\pm\sqrt{5})/2$.

12.103 $1\pm i$; $(-1\pm\sqrt{21})/2$.

第十三章　形式语言、形式语法和自动机

13.1　引　言

人们可以把一个数字计算机看成一种机器 M，它具有如下特性：在计算的每一步中，M 处于某种内部状态，M 读进输入，打印出输出，而输出仅仅依赖于 M 的内部状态和输入，然后，可能的话，M 改变它的内部状态. 有许多方法来定义机器 M，且 M 具有一定的结构.

人们通过一种特殊的机器 M(Turing 机)来定义可计算的函数. 这种特殊的机器可以由输入的非负整数 n 产生出一非负整数 $M(n)$ 输出. 非负整数能把绝大多数的数据、信息编码，因而这种机器 M 可以处理绝大多数的数据、信息.

本章将讨论这些及相关问题.

13.2　字母表，字符串，自由半群

考虑一非空符号集合 A，集合 A 上的字符串 w 是 A 中元素的有限序列. 例如，

$$u = ababb \quad \text{和} \; v = accbaaa.$$

这些序列是集合 $A=\{a,b,c\}$ 上的字符串. 当我们讨论 A 中字符串时，我们通常称 A 为字母表，它的元素称为字符. 我们也可以作这样的简写：把 aa 写成 a^2，aaa 写成 a^3，等等. 因而，上面的字符串也可以写成

$$u = abab^2, \; v = ac^2ba^3.$$

没有字符的序列，可用 λ(希腊字母，(lmbda)或 ε(希腊字母 epsilon)或 1 来表示，也可以看成是 A 的字符串，叫做空串. A 中所有字符串的集合记为 A^*.

字符串 u 的长度记作 $|u|$ 或 $l(u)$，它表示字符串 u 中字符的个数. 对于上述的 u，v，$l(u)=5$，$l(v)=7$，$l(\lambda)=0$. 这里 λ 是空串.

注　如不作其他说明，则字母表 A 是有限的，符号 u，v，w 将用来表示 A 中的字符串，A 中的字符用 a，b，c 表示.

连接

考虑 A 中的两个字符串 u 和 v. 连接 u 和 v 记作 uv，它表示字符串 v 紧接着写在字符串 u 之后. 以上面的 u 和 v 为例

$$uv = ababbaccbaaa = abab^2ac^2ba^3.$$

我们定义 $u^2=uu$，$u^3=uuu$. 一般地，$u^{n+1}=uu^n$，这里 u 是一个字符串.

显然，对于任意字符串 u，v，w，$(uv)w$ 和 $u(vw)$ 是一样的. 它们简单地以字符串 u，v，w 一个接一个地组合在一起. 而且，字符串 u 之前或之后连接一空串并不改变字符串 u. 换句话说：

定理 13.1　字母表 A 中的字符串的连接运算满足结合律，空串 λ 是运算中的单位元.
(一般来说，运算的交换律不成立. 例如，$uv \neq vu$)

子串，前缀

考虑字母表中任意字符串 $u=a_1a_2\cdots a_n$，任何序列 $w=a_ja_{j+1}\cdots a_k$ 称作 u 的子串. 特别地，子串 $w=a_1a_2\cdots a_k$，以 u 开始的字符开头，称作 u 的前缀. 换句话说，如果 $u=v_1wv_2$，则 w 是 u 的子串，且如果 $u=wv$，则 w 是 u 的前缀. 注意，λ 和 u 同时是 u 的子串，因为 $u=\lambda u$.

考虑字符串 $u=abca$，u 的子串和前缀如下：

(1) 子串：λ，a，b，c，ab，bc，ca，abc，bca，$abca$.

(2) 前缀：λ，a，ab，abc，$abca$.

注意,子串 $w=a$ 在 u 中出现在两个地方;字符串 ac 不是 u 的子串,尽管它所有的字符都属于 u.

自由半群,自由幺半群

用 F 表示字母表 A 中所有非空字符串的集合,并且含有连接运算.如前文所述,连接运算满足结合律.因此 F 是一个半群.称作 A 的*自由半群*或*由 A 生成的自由半群*.人们很容易证明 F 满足左右消去律.然而,当 A 中有多于一个元素时,F 不满足交换律.

当我们要标明集合 A 时,A 的自由半群记作 F_A.

现设 $M=A^*$ 是包括空串 λ 在内的 A 中所有字符串的集合.由于 λ 是连接运算的单位元,M 是含幺半群,我们称 M 为 A 上的*自由幺半群*.

13.3 形式语言

字母表 A 上的*形式语言* L 是 A 中字符串的集合.回顾 A^* 表示 A 中所有字符串的集合.因此,形式语言 L 是 A^* 的一个子集.

例 13.1 设 $A=\{a,b\}$,下面是 A 的形式语言:

(a) $L_1=\{a,ab,ab^2\cdots\}$,

(b) $L_2=\{a^mb^n:m>0,n>0\}$,

(c) $L_3=\{a^mb^m:m>0\}$,

(d) $L_4=\{b^mab^n:m\geq 0,n\geq 0\}$.

可以如下描述这些形式语言:

(a) L_1 由所有以 a 开头且由 0 个或 0 个以上个 b 跟随的字符串构成.

(b) L_2 由所有以 1 个或 1 个以上个 a 开头且由 1 个或 1 个以上个 b 跟随的字符串构成.

(c) L_3 由所有以 1 个或 1 个以上个 a 开头且由与 a 相同数量的 b 跟随的字符串构成.

(d) L_4 由所有只含有一个 a 的字符串构成.

形式语言的运算

假设 L 和 M 是 A 的形式语言,那么 L 和 M 的"连接",记为 LM,是 A 上的一种形式语言,其定义如下:

$$LM=\{uv:u\in L,v\in M\}.$$

即 LM 表示 L 中的字符串与 M 中的字符串经过连接而形成的字符串的全体.例如,假设

$$L_1=\{a,b^2\},\ L_2=\{a^2,ab,b^3\},\ L_3=\{a^2,a^4,a^6,\cdots\}.$$

那么,

$$L_1L_2=\{a^3,a^2b,ab^3,b^2a^2,b^2ab,b^5\},$$

$$L_1L_3=\{a^3,a^5,a^7,\cdots,b^2a^2,b^2a^4,b^2a^6,\cdots\},$$

$$L_1L_1=\{a^2,ab^2,b^2a,b^4\}.$$

明显地,形式语言的连接满足结合律,因为字符串的连接满足结合律.

形式语言 L 的幂定义如下:

$$L^0=\{\lambda\},\ L^1=L,\ L^2=LL,\ L^{m+1}=L^mL(m>1).$$

一元运算 L^*(读作"L 星")称作 L 的 *Kleene 闭包*,因为 Kleene 证明了定理 13.2,并定义了如下的并集

$$L^*=L^0\cup L^1\cup L^2\cup\cdots=\bigcup_{k=0}^{\infty}L^k$$

L^* 的定义与 A^* 一致,即由 A 的所有字符串构成.一些教科书定义 L^+ 为 $L^1,L^2,\cdots$ 的并集,也就是说 L^+ 与 L^* 一样,但 L^+ 不包括空串 λ.

13.4 正则表达,正则语言

设 A 是一(非空)字母表.本节定义 A 上的正则表达 r 及与 r 相关的正则语言 $L(r)$. 正则表达 r 和它对应的正则语言 $L(r)$ 归纳定义如下:

定义 下面每一项均为字母表 A 中的正则表达:

(1) 符号 λ(空串)和括号( )(空表达)是正则表达.

(2) A 中每个字母 a 是正则表达.

(3) 如果 r 是正则表达,那么 (r^*) 是正则表达.

(4) 如果 r_1 和 r_2 是正则表达,那么 $(r_1 \vee r_2)$ 是正则表达.

(5) 如果 r_1 和 r_2 是正则表达,那么 $(r_1 r_2)$ 是正则表达.

所有正则表达以上面的五种形式组成.

注意:正则表达 r 是一种特殊的字符串,它用 A 中字符和如下五种符号:

$$(\quad) \quad * \quad \vee \quad \lambda$$

我们强调,没有其他符号用于正则表达.

定义 A 上的形式语言 $L(r)$ 由正则表达 r 定义如下:

(1) $L(\lambda)=\{\lambda\}$ 和 $L(())=\varnothing$,空集.

(2) $L(a)=\{a\}$,其中 a 是 A 中字符.

(3) $L(r^*)=(L(r))^*$ [$L(r)$ 的 Kleene 闭包]

(4) $L(r_1 \vee r_2)=L(r_1)\cup L(r_2)$ (形式语言的并集)

(5) $L(r_1 r_2)=L(r_1)L(r_2)$ (形式语言的连接)

注 因为形式语言的连接和并满足结合律,而且"*"运算优先于连接,连接先于"∨",所以许多括号可以省去.

定义 设 L 为 A 上的形式语言.若存在 A 上的一正则表达 r 使得 $L=L(r)$,则 L 称为 A 的正则语言.

例 13.2 设 $A=\{a,b\}$. 下面是表达 r 和它对应的语言 $L(r)$:

(a) $r=a^*$,则 $L(r)$ 由所有 a 的幂组成,即 a 组成的所有字符串(包括空串 λ).

(b) $r=aa^*$,则 $L(r)$ 由所有 a 的幂组成,即 a 组成的除空串外的所有字符串.

(c) $r=a\vee b^*$,则 $L(r)$ 由 a 或 b 的幂组成,即

$$L(r) = \{a,\lambda,b,b^2,\cdots\}.$$

(d) $r=(a\vee b)^*$ 由 $L(a\vee b)=\{a\}\cup\{b\}=A$,因此 $L(r)=A^*$ 是 A 中所有字符串.

(e) $r=(a\vee b)^*bb$,则 $L(r)$ 由 A 中任意字符串与 bb 连结所形成的字符串组成.

(f) $r=a\wedge b^*$. $L(r)$ 不存在,因为 r 不是正则表达.($\wedge$ 不是正则表达的符号.)

例 13.3 考虑如下形式语言,其中 $A=\{a,b\}$.

(a) $L_1=\{a^m b^n : m>0, n>0\}$.

(b) $L_2=\{b^m a b^n : m>0, n>0\}$.

(c) $L_3=\{a^m b^m : m>0\}$.

找出 $A=\{a,b\}$ 中的正则表达 r,使得 $L_i=L(r)$ $(i=1,2,3)$.

(a) L_1 由以大于等于 1 个 a 开头且被大于等于 1 个 b 跟随的字符串组成. 因此我们可以写成 $r=aa^*bb^*$. 注意:r 不是惟一的. 例如,$r=a^*abb^*$ 就是另一种解.

(b) L_2 由所有这样的字符串组成:以大于等于 1 个 b 开头,紧跟一个 a 再跟大于等于 1 个 b,即所有的字符串仅有一个 a,它既不是第一个字母,也不是最后一个. 因此 $r=bb^*abb^*$ 是一个解.

(c) L_3 由所有这样的字符串组成:以大于等于 1 个的 a 开头并以与其相同数量的 b 跟随. 不存在正则表达 r,使得 $L_3=L(r)$,即 L_3 不是正则语言. 这个事实的论证见例 13.7.

13.5 有限自动机

有限自动机(FSA),或者简单地说自动机 M,由下述五部分组成:

(1) 一个有限的输入集合 A(字母表).

(2) (内部的)一个有限状态集合 S.

(3) S 的一个子集 Y(Y 的元素称为接受状态).

(4) S 中的初始状态 s_0.

(5) S 中的状态转移函数 $F:S\times A\to S$.

当我们要指明它的五部分时,自动机 M 被记为 $M=(A,S,Y,s_0,F)$

在有的书中,状态转移函数 $F:S\times A\to S$ 定义为:对每一个 $a\in A$,定义 $f_a:S\to S$;即每一个输入 a 可看作引起自动机 M 的状态改变. 置 $F(s,a)=f_a(s)$ 表明两个定义是等价的.

例 13.4 下面是用两个输入符号和三个状态定义的自动机 M

(1) $A=\{a,b\}$,输入符号.

(2) $S=\{s_0,s_1,s_2\}$,内部状态.

(3) $Y=\{s_0,s_1\}$,接受状态.

(4) s_0 初始状态.

(5) 状态转移函数 $F:S\times A\to S$ 定义如下:

$$F(s_0,a)=s_0,\ F(s_1,a)=s_0,\ F(s_2,a)=s_2,$$
$$F(s_0,b)-s_1,\ F(s_1,b)=s_2,\ F(s_2,b)=s_2.$$

这种状态转移函数 F 经常以表格的形式给出,如图 13-1

F	a	b
s_0	s_0	s_1
s_1	s_0	s_2
s_2	s_2	s_2

图 13-1

自动机 M 的状态图

自动机通常用它的状态图 $D=D(M)$ 来定义,而不是列出它的五个部分. 状态图 $D=D(M)$ 是如下的一种带标记的有向图.

(1) $D(M)$ 的结点是 S 的状态,接受状态用双圈表示.

(2) 在 $D(M)$ 中,若 $F(s_j,a)=s_k$ 或 $f_a(s_j)=s_k$,则用一个标有输入 a 的箭头从 s_j 指向 s_k.

(3) 初始状态 s_0 是通过一特殊的箭号表示,这个箭号终止于 s_0. 但是没有初始结点.

对于每一个结点 s_j 和在字母表 A 中每个字符 a,都有一个标有 a 的箭头从 s_j 出发;因此每个结点出发的度数与 A 中元素的个数是相等的. 为简便计,我们可以用单独的一个箭头标明那些引起相同的状态变化的输入,而不是一个输入用一个箭头.

例 13.1 中自动机 M 的状态图可表示为图 13-2. 注意,标有 a 和 b 的箭头,从 s_2 到 s_2,因为 $F(s_2,a)=s_2$ 且 $F(s_2,b)=s_2$. 同时注意结点的出发度数为 2.

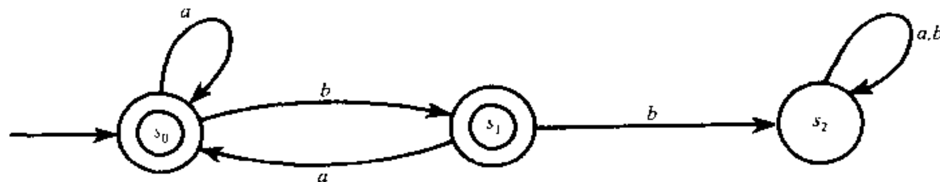


图 13-2

自动机 M 决定的形式语言 $L(M)$

每一个有输入字母表 A 的自动机 M 定义 A 上的一种形式语言 $L(M)$ 如下：

设 $w=a_1a_2\cdots a_m$ 为 A 中的一字符串，则 w 确定一状态序列：

$$s_0 \to s_1 \to s_2 \to \cdots \to s_m.$$

其中 s_0 为初始状态且 $F(s_{i-1},a_i)=s_i(i\geqslant 1)$. 换句话说，$w$ 确定了状态图 $D(M)$ 的路径：

$$P=(s_0,a_1,s_1,a_2,s_2,\cdots,a_m,s_m).$$

如果最后状态 s_m 是 Y 中的接受状态则说 M 识别字符串 w.

M 的形式语言 $L(M)$ 为 A 中被 M 接受的所有字符串的集合.

例 13.5 (a) 判定图 13-2 中的自动机 M 是否接受字符串 w：

(1) $w=ababba$；(2) $w=baab$；(3) $w=\lambda$.

(1) 利用图 13-2，字符串 $w=ababba$ 获得路径

$$P=s_0\xrightarrow{a}s_0\xrightarrow{b}s_1\xrightarrow{a}s_0\xrightarrow{b}s_1\xrightarrow{b}s_2\xrightarrow{a}s_2.$$

最后状态 s_2 不在 Y 中，因此 M 不接受 w.

(2) 字符串 $w=baab$ 确定如下路径

$$P=s_0\xrightarrow{b}s_1\xrightarrow{a}s_0\xrightarrow{a}s_0\xrightarrow{b}s_1.$$

最后状态 s_1 在 Y 中，因此 M 接受 w.

(3) 因为 w 是空串，所以最后状态即初始状态 s_0. 因为 s_0 属于 Y，所以 M 接受 λ.

(b) 根据图 13-2 描述自动机 M 的形式语言 $L(M)$.

$L(M)$ 由 A 中所有没有连续两个 b 的字符串组成. 这来自于下面的事实：

(1) 我们只有在连续的两个 b 之后进入 s_2 状态.

(2) 我们不可能离开 s_2.

(3) s_2 状态是惟一的拒绝（不接受）状态.

正则语言和自动机之间最基本的关系包含在下面的定理中.（其证明超出了本书的范围）

定理 13.2 (Kleene) 字母表 A 上的形式语言 L 是正则的当且仅当存在一个有穷自动机 M 使得 $L=L(M)$.

在形式语言 L 上的 * 运算 L^* 有时称作 L 的 Kleene 闭包，因为 Kleene 第一个证明了上面的基本结果.

例 13.6 设 $A=\{a,b\}$，构造一个自动机 M 使之恰好接受 A 中以两个 b 结尾的字符串.

因为 b^2 被接受，而 λ 或 b 不能. 因此需要三个状态：s_0（初始状态），s_1 和 s_2 且带有标有 b 的从 s_0 到 s_1 和从 s_1 到 s_2 的两个箭头. 而且，s_2 是一个接受状态且 s_0 和 s_1 不是. 这在图 13-3(a)中给出. 另一方面，如果有一个 a，那么我们就要回到 s_0. 如果我们在 s_2 上有一个 b，那么我们就要停留在 s_2. 这些附加的条件给出了我们所需要的自动机 M，见图 13-3(b).

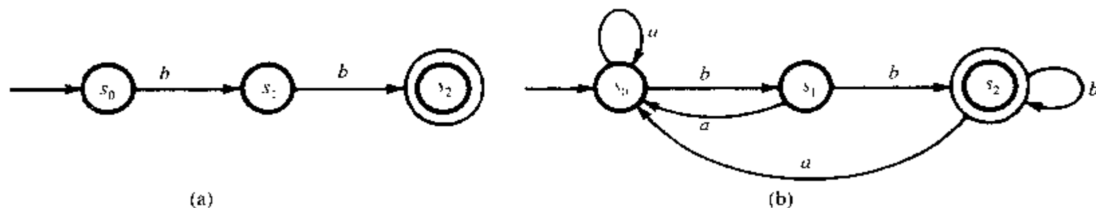


图 13-3

Pumping 引理

假设 A 上的自动机 M 有 k 个状态，并假设 $w=a_1a_2\cdots a_n$ 是被 M 接受的 A 上的字符串满足 $|w|=n>k$. 设

$$P=(s_0,s_1,\cdots,s_n)$$

为字符串 w 对应的状态序列. 因为 $n>k$，所以 P 中有两种状态应是相同的，即 $s_i=s_j$ $(i<j)$. 设 $x=a_1a_2\cdots a_i$, $y=a_{i+1}\cdots a_j$, $z=a_{j+1}\cdots a_n$，如图 13－4 所示，xy 以 $s_i=s_j$ 结尾，因此 xy^m 也以 s_i 结尾. 因而，对于每一个 m，$w_m=xy^mz$ 以 s_n 结尾，s_n 是一个接受状态.

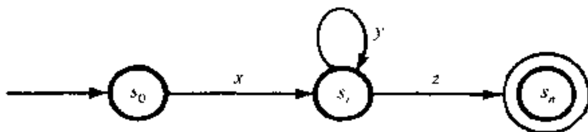


图 13－4

以上的讨论证明了下面的重要结论.

定理 13.3（Pumping 引理） 假设 M 是 A 上的自动机并满足：

(i) M 有 k 个状态.

(ii) M 接受 A 的字符串 w，这里 $|w|>k$.

那么 $w=xyz$，这里对每一个正整数 m，$w_m=xy^mz$ 被 M 接受.

下一个例子是关于 Pumping 引理的应用.

例 13.7 证明形式语言 $L=\{a^mb^m : m>0\}$ 是不正则的.

假设 L 是正则的. 那么，根据定理 13.2，存在有限自动机 M 且 M 接受 L. 假设 M 有 k 个状态. 令 $w=a^kb^k$，则 $|w|>k$. 根据 Pumping 引理(定理 13.3)，$w=xyz$，其中 y 非空且 $w_2=xy^2z$ 也被 M 接受. 如果 y 仅由 a 或 b 组成，那么 w_2 将不会有与 b 相同数目的 a. 如果 y 同时含有 a 和 b，那么 w_2 将含有 a 跟随 b. 在两种情况下，w_2 都不属于 L，这是一个矛盾. 因此 L 不是正则的.

13.6 形式语法

图 13－5 所示的是一个句子的语法结构：

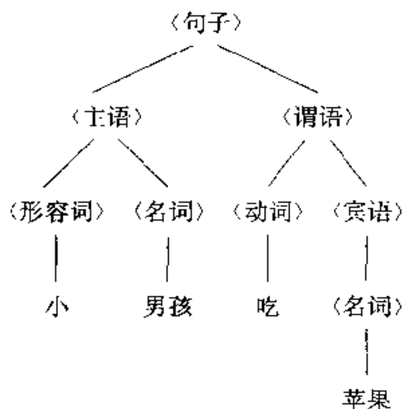


图 13－5

(1) 各种变元，例如，〈句子〉，〈名词短语〉，…；

(2) 各种终结符，例如，"男孩"，"苹果"，…；

(3) 起始变元〈句子〉；

(4) 各种产生式，例如

〈句子〉→〈名词短语〉〈动词短语〉

〈宾语短语〉→〈名词〉

〈名词〉→苹果

最后的句子仅包含了终结符，尽管变元和终结符二者都通过产生式出现在结构中. 这种直观的描述是为了定义下面将出现的形式语法及其生成的形式语言.

一个*短语结构形式语法*，简称*形式语法* G，由四个部分构成：

(1) 一个有限集(词汇)V.

(2) V 的一个子集 T，T 的元素称为*终结元*；集合 $N=V\backslash T$ 的元素称为*非终结元*或*变元*.

(3) 一个非终结符 S 称为*起始符*.

(4) 一个产生式的有限集 P. 产生式是一个有序偶(α,β)，通常记作 $\alpha\to\beta$，其中 α、β 是 V 上的字符串. P 中每个产生式的左端必须至少包括一个非终结元.

这样的一个形式语法 G，记作 $G=G(V,T,S,P)$.

除特别说明或暗示外，形式语法用下面的记法：终结元用斜体小写拉丁字母 $a,b,c,\cdots$ 表示；非终结元用斜体大写拉丁字母 $A,B,C,\cdots$ 表示；起始符用 S 表示. 同时，V 中的字符串，即终结元或非终结元的字符串用希腊字母 $\alpha,\beta,\cdots$ 来表示. 此外，我们将

$$\alpha\to\beta_1,\ \alpha\to\beta_2,\ \cdots,\ \alpha\to\beta_k，\text{记作}:\alpha\to(\beta_1,\beta_2,\cdots\beta_k).$$

注　一般地，我们只根据给出的产生式来定义一个形式语法 G，并默认 S 是初始符，G 中的终结元和非终结元只在产生式中出现.

例 13.8　形式语法 G 定义如下：

$$V=\{A,B,S,a,b\},\ T=\{a,b\},$$

$$P=\{S\xrightarrow{1}AB,\ A\xrightarrow{2}Aa,\ B\xrightarrow{3}Bb,\ A\xrightarrow{4}a,\ B\xrightarrow{5}b\}.$$

其中 S 是初始符. 产生式可缩写成

$$S\to AB,\ A\to(Aa,a),\ B\to(Bb,b).$$

形式语法 G 的形式语言 $L(G)$

假定 w 和 w' 是形式语法 G 的词汇集合 V 上的字符串. 我们写成

$$w\Rightarrow w'.$$

如果 w' 能够由 w 通过使用一个产生式得到；即，如果存在字符串 u 和 v 使 $w=u\alpha v$ 且 $w'=u\beta v$，并且有一个产生式 $\alpha\to\beta$. 我们写成

$$w\Rightarrow\Rightarrow w'\quad\text{或}\quad w^*\Rightarrow w'.$$

如果 w' 能够由 w 通过使用有限个产生式得到.

设 G 是一个形式语法，T 是 G 的终结元集. G 的形式语言，记作 $L(G)$，由初始符 S 通过以上过程得到 T 上的字符串组成. 即：

$$L(G)=\{w\in T^*:s\Rightarrow\Rightarrow w\}$$

例 13.9　考虑例 13.8 中的形式语法 G. 观察到 $w=a^2b^4$ 可由初始符 S 通过如下过程得到：

$$S\Rightarrow AB\Rightarrow AaB\Rightarrow aaB\Rightarrow aaBb\Rightarrow aaBbb\Rightarrow aaBbbb\Rightarrow aabbbb=a^2b^4.$$

这里分别使用了产生式 1,2,4,3,3,3,5. 所以可以写成 $S\Rightarrow\Rightarrow a^2b^4$. 因此 $w=a^2b^4$ 属于 $L(G)$. 更一般地，产生式序列 1,2(r 次),4,3(s 次),5 能生成字符串 $w=a^rab^sb$，其中 r 和 s 是非负整数. 另一方面，没有一个产生式序列能生成 b 后面的 a. 从而，

$$L(G)=\{a^mb^n:m\text{ 和 }n\text{ 是正整数}\}.$$

即形式语法 G 的形式语言 $L(G)$ 由所有这样的字符串组成：字符串以一个或几个 a 开头，a 后跟有一个 b 或几个 b.

例 13.10　找出由带有如下产生式的形式语法 G 形成的$\{a,b,c\}$上的形式语言 $L(G)$.

$$S\to aSb,\ aS\to Aa,\ Aab\to c.$$

首先使用第一个产生式一次或多次，得到字符串 $w=a^nSb^n$，其中$n>0$，为了消去 S，必须使用第二个产生式，得到字符串 $w'=a^mAabb^m$，其中$m=n-1\geq 0$. 现在我们只能用第三个产生式，最终得到字符串 $w''=a^mcb^m$，其中 $m\geq 0$. 因此

$$L(G)=\{a^mcb^m;m \text{ 是非负整数}\}.$$

即形式语言 $L(G)$由所有这样的字符串组成：字符串由被 c 隔开的相同非负个数的 a 和 b 构成.

形式语法的类型

形式语法根据所允许的产生式的种类来分类. 下面是 Noam Chomsky 提出的形式语法分类法：

一个 0 型形式语法在产生式上没有限制. 第 1,2,3 类型定义如下：

(1) 一个形式语法 G 是第一类型，如果它所有的产生式都是 $\alpha\to\beta$(其中$|\alpha|\leq|\beta|$)形式或 $\alpha\to\lambda$ 形式.

(2) 一个形式语法 G 是第二类型，如果它所有的产生式都是 $A\to\beta$，(即其中左端是一个非终结元)形式.

(3) 一个形式语法 G 是第三类型，如果它所有的产生式都是这样的形式：$A\to a$ 或$A\to aB$，(即左端是一个非终结元、右端是一个终结元或一个终结元后跟一个非终结元)，或 $S\to\lambda$ 形式.

可以看出，形式语法形成一个阶层组织；即第三类型形式语法都是第二类型形式语法，第二类型形式语法都是第一类型形式语法，第一类型形式语法都是 0 类型形式语法.

形式语法也可以分类成上下文有关的语法、上下文无关的语法、正则的语法：

(a) 一个形式语法 G 是上下文有关的，如果它的产生式都是这样的形式

$$\alpha A\alpha'\to\alpha\beta\alpha'.$$

称它为“上下文有关的”是因为只有当变元 A 在 α 与 α'之间时，才总可以用 β 来取代 A.

(b) 一个形式语法 G 是上下文无关的，如果它的产生式都是这样的形式

$$A\to\beta.$$

称它为“上下文无关的”是因为无论变元 A 在什么位置，我们总可以用 β 来取代 A.

(c) 一个形式语法是正则的，如果它的产生式是这样的形式：

$$A\to a,\ A\to aB,\ S\to\lambda.$$

可以看出，上下文无关的形式语法与第二类型形式语法是等价的，正则形式语法与第三类型形式语法是等价的.

下面是正则形式语法与有限自动机的基本关系.

定理 13.4 形式语言 L 能由第三类型(正则)形式语法 G 生成，当且仅当存在一个有限自动机 M 能够接受 L.

因此，一个形式语言 L 是正则的，当且仅当 $L=L(r)$，其中 r 是正则表达；当且仅当 $L=L(M)$，其中 M 是有限自动机；当且仅当 $L=L(G)$，其中 G 是正则形式语法.

例 13.11 考虑形式语言 $L=\{a^nb^n;n>0\}$.

(a) 找出一个生成 L 的上下文无关的形式语法 G. 显然，带有如下产生式的形式语法 G 将生成 L

$$S\to ab,\ S\to aSb.$$

注意，G 是一个上下文无关的形式语法，因为每个左端都是一个非终结元.

(b) 找出一个生成 L 的正则形式语法 G.

根据例 13.7，L 不是正则形式语言，因此 L 不能由正则形式语法生成.

上下文无关语法的导出树

考虑一个上下文无关的(第 2 型)形式语法 G. $L(G)$中的字符串 w 的导出可以用有序、有

根的树 T 来形象地描述，称为导出树. 例如，设 G 是一个带有如下产生式的上下文无关的形式语法：

$$S \to aAB,\ A \to Bba,\ B \to bB,\ B \to c.$$

字符串 $w=acbabc$ 可由 S 这样得到：

$$S \Rightarrow aAB \to a(Bba)B \to acbaB \to acba(bB) \Rightarrow acbabc.$$

可以如图 13-6 来画导出树. 特别地，我们以 S 作为根，然后根据在导出 w 时所用到的产生式来添加枝条. 这样得到的完整的导出树如图 13-6(e)所示. T 中从左到右的叶序列就是导出的字符串 w. 而 T 中不是叶的是变元，如 A，A 的直接继元(孩子们)形成一个字符串 α，其中 $A \to \alpha$ 是在 w 的导出中用过的 G 的产生式.

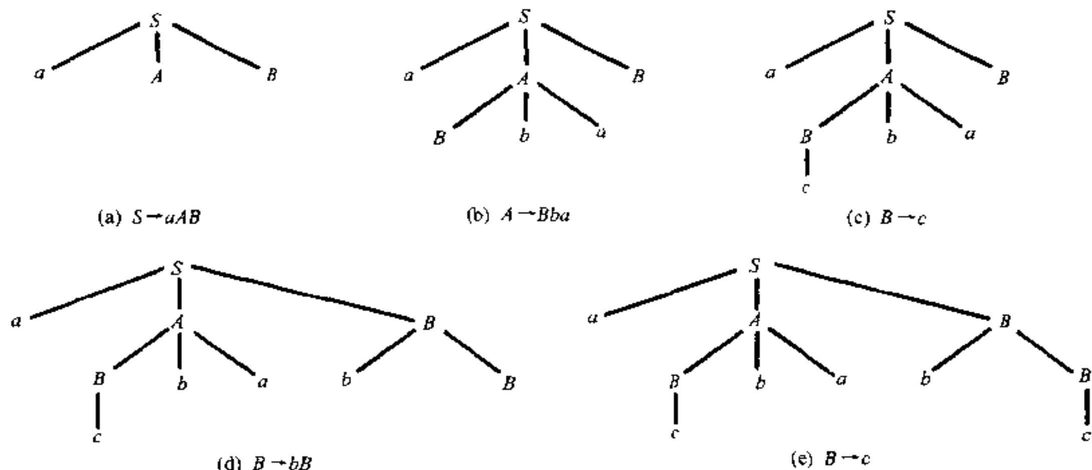


图 13-6

Backus-Naur 形式

在描述上下文无关的(第 2 类型)形式语法的产生式时，有时也用另外一种记法，称作 Backus-Naur 形式. 它的不同之处在于：

(i) 不用→而用∷=.

(ii) 非终结元要用⟨ ⟩括起来.

(iii) 所有左端有相同非终结元的产生式要合并成一句，所有的右端在∷=的右边列出，并用短竖隔开.

例如，产生式 $A \to aB$，$A \to b$，$A \to BC$ 合并成一句

$$\langle A\rangle ::= a\langle B\rangle \mid b \mid \langle B\rangle\langle C\rangle.$$

自动机与形式语法

定理 13.4 告诉我们，正则形式语法对应的有限状态自动机(FSA). 还有其他比 FSA 功能更强的自动机，对应其他形式语法.

(a) Pushdown 自动机　Pushdown 自动机 P 与 FSA 类似，且 P 有一个辅助储存器能为它提供无限大容量的存储空间. 形式语言 L 能被 Pushdown 自动机识别，当且仅当 L 是上下文无关的形式语言.

(b) 线性有界自动机　线性有界自动机 B 比 Pushdown 自动机的功能更强，这样的自动机 B 使用一种带子，这种带子是根据输入字符串 w 的字长而线性有界的. 形式语言 L 能被自动机 B 识别当且仅当 L 是上下文有关的.

(c) Turing 自动机　Turing 自动机 M，是以英国数学家 Alan Turing 的名字命名的. 它使用的是一种无限长的带子. 它能识别由任何短语结构形式语法 G 生成的所有形式语言. 事

实上，Turing 自动机 M 是一系列定义可数函数的等价方法中的一种.

对 Pushdown 自动机与线性有界自动机的讨论已超出了本书的范围. 我们将在 13.8 节讨论 Turing 自动机.

13.7 有限状态机

有限状态机(FSM)与有限状态自动机(FSA)类似，只是 FSM 输出时使用一种与输入字母表不同的输出字母表. 正式定义如下：

有限状态机(或完全序列机)M 由六个部分组成：

(1) 一个输入符的有限集 A.

(2) 一个内部状态的有限集 S.

(3) 一个输出符的有限集 Z.

(4) S 中的一个初始状态 s_0.

(5) 一个从 $S\times A$ 到 S 状态转移函数 f.

(6) 一个从 $S\times A$ 到 Z 的输出函数 g.

这样的一个机器 M 被记作 $M=M(A,S,Z,s_0,f,g)$，表示它的六个部分.

例 13.12 下面定义了一个有限状态机 M，有两个输入符，三个内部状态、及三个输出符：

(1) $A=\{a,b\}$.

(2) $S=\{s_0, s_1, s_2\}$.

(3) $Z=\{x,y,z\}$.

(4) 初始状态 s_0.

(5) 状态转移函数 $f:S\times A\to S$，定义如下：

$$f(s_0,a)=s_1,\ f(s_1,a)=s_2,\ f(s_2,a)=s_0,$$
$$f(s_0,b)=s_2,\ f(s_1,b)=s_1,\ f(s_2,b)=s_1.$$

(6) 输出函数 $g:S\times A\to S$，定义如下：

$$g(s_0,a)=x,\ g(s_1,a)=x,\ g(s_2,a)=z,$$
$$g(s_0,b)=y,\ g(s_1,b)=z,\ f(s_2,b)=y.$$

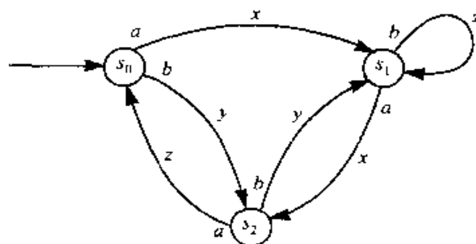
有限状态机的状态表与状态图

要以紧凑的形式来描述一个有限状态机有两种方法. 一种是用表格，称作有限状态机 M 的状态表，另一种是用有标记的有向图，称作有限状态机的状态图.

状态表把状态转移函数 f 与输出函数 g 放在同一个表格内，这个表格描述了由 $F(s_i,a_j)=(f(s_i,a_j),g(s_i,a_j))$ 定义的函数 $F:S\times A\to S\times Z$. 例如，例 13.12 中有限状态自动机的状态表如图 13-7(a)所示. 从初始状态开始，状态列在表的左方，输入符列在表的上方. 表中的元素，是一个对子(s_k,z_r)，其中 $s_k=f(s_i,a_j)$是下一状态，$z_r=g(s_i,a_j)$是输出符. 我们假设除了出现在表中的输出符之外没有其他的输出符.

F	a	b
s_0	s_1,x	s_2,y
s_1	s_2,x	s_1,y
s_2	s_0,x	s_1,y

(a)



(b)

图 13-7

有限状态机 $M=M(A,S,Z,s_0,f,g)$的状态图 $D=D(M)$是一个有标记的有向图. D 的结

点是M的状态.此外,如果

$$F(s_i,a_j)=(s_k,z_r),\text{ 即 } f(s_i,a_j)=s_k \text{ 且 } g(s_i,a_j)=z_r.$$

那么,从s_i到s_k就有一条标着a_j和z_r的箭头.我们通常放输入符a_j靠近箭头的始端(靠近s_i),输出符z_r靠近箭头的中心.我们还通过另外画一条指向s_0的箭头来标记初始状态s_0.例如,例13.12中有限状态机M的状态图如图13-7(b)所示.

输入与输出带

上面对于有限自动机M的讨论还没有显示出M的动态特征.假定给M一个输入符的字符串,如

$$u=a_1a_2\cdots a_m.$$

我们设想这些符号在一条"输入带"上,机器M一个一个地读这些输入符,同时进行一系列的状态转换

$$V=s_0s_1s_2\cdots s_m.$$

其中s_0是初始状态,并且把输出符的字符串

$$w=z_1z_2\cdots z_m.$$

打印在一条"输出带"上.准确地说,初始状态s_0和输入字符串u通过

$$s_i=f(s_{i-1},a_i)\quad \text{和}\quad z_i=g(s_{i-1},a_i)$$

来决定字符串v和w.其中$i=1,2,\cdots,m$.

例 13.13　考虑图13-7即例13.12中有限状态机.假定输入一个字符串$u=abaab$,下面我们从状态图中计算状态序列v和输出字符串w.从初始状态s_0开始,我们随着被输入符标记如下的箭头

$$s_0\xrightarrow{a,x}s_1\xrightarrow{b,z}s_1\xrightarrow{a,x}s_2\xrightarrow{a,z}s_0\xrightarrow{b,y}s_2.$$

就得到如下的序列v和输出字符串w

$$v=s_0s_1s_1s_2s_0s_2\quad \text{和}\quad w=xzxzy.$$

二进制加法

这里介绍能做二进制加法的有限状态机.通过在数据的首端补0,我们可以认为数据有相同的二进制数位.如果给机器输入

$$\begin{array}{r}1101011\\ \underline{+0111011}\end{array}$$

那么输出的和应是二进制数

$$10100110.$$

具体地说输入是一串待加的二进制数对

$$11,11,00,11,01,11,10,b.$$

其中b表示空格,那么输出应是一串

$$0,1,1,0,0,1,0,1.$$

我们还希望机器做完加法后就进入"停止"状态.输入符是

$$A=\{00,01,10,11,b\}.$$

输出符就是

$$Z=\{0,1,b\}.$$

我们所"建造"的机器有三种状态

$$S=\{\text{执行}(c),\text{初始}(n),\text{停止}(s)\}.$$

这里n是初始状态.机器如图13-8所示.

为了说明这种机器的局限性，我们有如下定理：

定理 13.5　没有一种有限状态机能做二进制乘法.

如果我们限制待乘数据的大小，那么这样的机器是存在的. 计算机是能做数据乘法的有限机的重要例子，但对数据大小有限制.

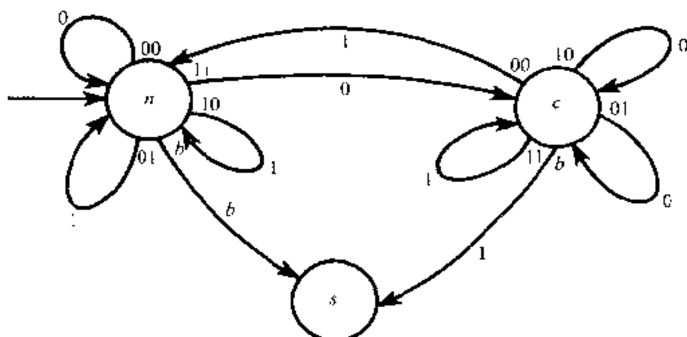


图 13-8

13.8　Gödel 数

回忆 11.5 节，一个正整数 $p(>1)$ 被称为素数，当且仅当它的正因数只有 1 和 p. 我们令 $p_1, p_2, \cdots$ 表示相继出现的素数. 那么

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ \cdots.$$

（根据定理 11.11，存在无限个素数）算术基本定理（定理 11.19）说明：任何正整数 $n(>1)$ 都能惟一地（除下顺序外）写成素数的乘积. 德国逻辑学家 Kurt Gödel 利用这个结果把数字的有限序列进行了编码，也把在有限或可数的字母表 A 上的字符串进行编码. 每个序列或字符串按下面规则对应的正整数，叫做 Gödel 数.

非负整数序列 $s=(n_1, n_2, \cdots, n_k)$ 的 Gödel 数是正整数 $c(s)$，其中 n_i 是 $c(s)$ 的素数分解式中 p_i 的指数，即

$$c(s) = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

例如，

$$c = \{3,1,2,0,2\}$$

被编码成

$$c(s) = 2^3 \cdot 3 \cdot 5^2 \cdot 7^0 \cdot 11^2 = 72\ 600,$$

字母表 $\{a_0,\ a_1,\ a_2,\ a_3,\ \cdots\}$ 上的字符串 w 的 Gödel 数是正整数 $c(w)$，其中 w 的第 i 个字母的下标是 $c(w)$ 的素数分解式中 p_i 的指数，如：

$$w = a_4 a_1 a_3 a_2 a_2$$

被编码成

$$c(w) = 2^4 \cdot 3 \cdot 5^3 \cdot 7^2 \cdot 11^2 = 35\ 574\ 000.$$

（可以看出两种编码本质上是一样的，因为我们可以将字符串 w 看成是它的字母的下标的序列）

上述编码过程实际上证明了本节的主要结论：

定理 13.6　如果字母表 A 是可数的，那么 A 上的所有形式语言 L 都是可数的.

证明　Gödel 编码是 1-1 映射 $c: L \to \mathbf{N}$，所以 L 是可数的.

13.9　Turing 机

正式定义一个"可数"函数有很多等价的方法. 我们用 Turing 机来定义它，本节正式定义 Turing 机，下一节将定义可数函数.

我们对 Turing 机的定义用了一个无限长的带子，五元组和三个停止状态. 其他定义用的是一个无限长的带和/或四元组和一个停止状态. 然而，所有的定义都是等价的.

基本定义

一个 Turing 机包括三个不交的非空集：

(1) 一个有限带集合

$$A = \{a_1, a_2, \cdots, a_m\} \cup \{B\}.$$

这里 $B = a_0$ 是"空格"符.

(2) 一个有限状态集

$$S = \{s_1, s_2, \cdots, s_n\} \cup \{s_0\} \cup \{s_H, s_Y, s_N\}.$$

这里 s_0 是初始状态. 另外，SH(HALT)是停止状态，SY(YES)是接受状态，SN(NO)是不接受状态.

(3) 一个有向集

$$d = \{L, R, N\}.$$

这里 L 表示"左"，R 表示"右"，N 表示"无运动"或"静止".

定义 13.1　一个表达是 $A \cup S \cup d$ 中的元素的一个有限(可能空)序列.

换句话说，一个表达就是一个字符串，字符串中的字母(符号)来自于集合 A、S 和 d.

定义 13.2　带表达是只使用带集 A 中元素的表达.

Turing 机 M 可看成是沿着一个无限长的带前后移动的读写头. 这个带被分成等长的小方格，每个小方格可以是空的或容有一个带符号. 每一步 Turing 机 M 处在某个内部状态 S_i，在带子上扫描某个带符号. 我们假定只有有限个非空符号出现在带子上.

图 13-9(a)是一个 Turing 机的示意图，这个 Turing 机处于 s_2 状态，正在扫描带子上的第二个符号，带子上印有 $a_1a_3Ba_1a_1$（再一次注意，B 是空格符）. 这个图形可用表达 $\alpha = a_1s_2a_3Ba_1a_1$ 来描述，这里我们把 M 的状态 s_2 写在 M 正在扫描的带符号 a_3 的前面. 注意到 α 是用带符号和状态符 s_2 表达的，s_2 不在表达的最后，因为它出现在带子正在扫描的带符号 a_3 的前面. 图 13-9 表明两个另外不常规的格局和它们相对应的格局表达.

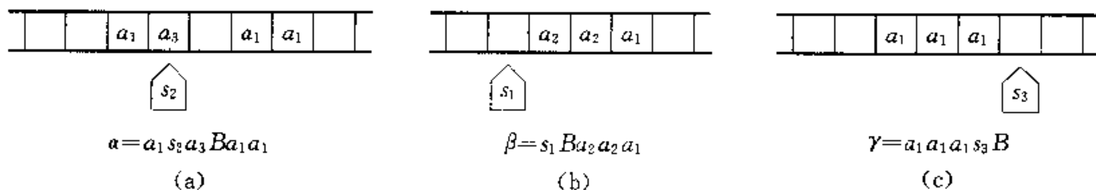


图 13-9

我们给出正式的定义.

定义 13.3　一个格局 α 是这样一个形状的表达

$$\alpha = Ps_ia_kQ.$$

此处的 P 和 Q 是线带的表达(可能是空的).

定义 13.4　设 $\alpha = Ps_ia_kQ$ 是一个格局. 我们说 Turing 机 M 处于 s_i 的状态，而 s_i 扫描字母 a_k，在线带上的表达是表达 Pa_kQ，也就是没有状态符号 s_i 的 α.

如上所述，Turing 机 M 每一步都及时地处于某个状态 s_i，同时扫描线带符号 a_k，Turing 机 M 能够同时完成下面三件事：

(i) M 可以擦去已输入的符号 a_k 而在这个位置上写上线带符号 a_l（此处我们允许 $a_l = a_k$）.

(ii) M 将它的内部状态 s_i 转变成状态 s_j（此处我们允许 $s_j = s_i$）.

(iii) M 向左移动一方格，向右移动一方格，或者根本就不动.

上述 M 作的行为我们可以用五个字母来表达，它被称作为一个五元组. 我们对它定义如

下：

定义 13.5 一个五元组 q 由如下形式的五个字母的表达

$$q=(s_i,a_k,a_l,s_j,\begin{Bmatrix}L\\R\\N\end{Bmatrix}).$$

也就是说，q 的第一个字母是一个状态符号，第二个是一个线带符号，第三个也是一个线带符号，第四个是一个状态符号，最后一个是方向符号 L，R 或 N.

下面我们给出 Turing 机的一个正式定义.

定义 13.6 Turing 机 M 是有限的五元组集合，满足：

(i) 没有两个五元组以相同的两个字母开始.

(ii) 没有一个五元组是以 s_H，s_Y 或 s_N 开始.

定义中的条件(i)保证了 M 在任一给定的步骤中最多只能做一件事，而条件(ii)保证了 M 机在状态 s_H，s_Y 或 s_N 下停止.

下面是另一个等价的定义.

定义 13.6′ Turing 机 M 是一个部分函数

$$S\backslash\{s_H,s_Y,s_N\}\times A\to A\times S\times d.$$

部分函数，简单地说，是表示 M 的定义域为 $S\backslash\{s_H,s_Y,s_N\}\times A$ 的子集.

对于上面所描述的 Turing 机的行为现在可正式地定义

定义 13.7 设 α 和 β 是两个格局. 我们写作

$$\alpha\to\beta,$$

如果下面中任何一个成立. 此处 a，b，c 是线带字母，而 P 和 Q 是线带表达(可能是空的)：

(i) $\alpha=Ps_iaQ$，$\beta=Ps_jbQ$ 和 M 包含着五元组 $q=s_iabs_jN$.

(ii) $\alpha=Ps_iacQ$，$\beta=Pbs_jcQ$ 和 M 包含着五元组 $q=s_iabs_jR$.

(iii) $\alpha=Pcs_iaQ$，$\beta=Ps_jcbQ$ 和 M 包含着五元组 $q=s_iabs_jL$.

(iv) $\alpha=Ps_ia$，$\beta=Pbs_jB$ 和 M 包含着五元组 $q=s_iabs_jR$.

(v) $\alpha=s_iaQ$，$\beta=s_jBbQ$ 和 M 包含着五元组 $q=s_iabs_jL$.

注意，在所有五种情况中，M 用 b 在线带中代替了 a(此处我们允许 $b=a$)，M 改变了它的状态，从 s_i 到 s_j(此处我们允许 $s_j=s_i$)，还有：

(i) 这里 M 不移动.

(ii) 这里 M 向右移动.

(iii) 这里 M 向左移动.

(iv) 这里 M 向右移动. 但是，因为 M 正扫描最右面的字母，它必须在右边加上空格符 B.

(v) 这里 M 向左移动. 但是，因为 M 正扫描最左面的字母，它必须在左边加上空格符 B.

定义 13.8 格局 α 是终止的，如果没有格局 β 使得 $\alpha\to\beta$.

特别地，处于三种停止状态中任何一种的格局 α 一定是终止的，因为没有一个五元组以 s_H，s_Y 或 s_N 开始.

用 Turing 机计算

上面是对 Turing 机 M 的一种静态描述(一步). 现在我们来讨论它的动态.

定义 13.9 Turing 机的一个计算是一列格局 $\alpha_0,\alpha_1,\cdots,\alpha_m$ 满足 $\alpha_{i-1}\to\alpha_i(i=1,\cdots,m)$ 以及 α_m 是终止的格局.

换句话说，一个计算是一个序列

$$\alpha_0\to\alpha_1\to\alpha_2\to\cdots\to\alpha_m.$$

这个序列不能再延续，因为 α_m 是终止的. 我们将用 $\mathrm{term}(\alpha)$ 来表示以 α 开始的计算的最后格局. 因此，在上面的计算中，$\mathrm{term}(\alpha_0)=\alpha_m$.

Turing 机的输入

定义 13.10　Turing 机 M 的一个输入是一个线带表达 W. 输入 W 的*初始格局*是 $\alpha(W)$. 此处 $\alpha(W)=s_0W$.

注意,输入 W 的最初格局 $\alpha(W)$ 是通过在输入线带表达 W 前放置最初状态 s_0 而获得的. 换句话说,Turing 机 M 在最初状态 s_0 开始,同时扫描 W 的第一个字母.

定义 13.11　设 M 是一个 Turing 机,W 是一个输入,如果有一个计算以初始格局 $\alpha(W)$ 开始,我们说 M *停止于* W 处.

也就是,给出一个输入 W,我们能形成初始格局 $\alpha(W)=s_0W$,并且应用 M 去获得一个序列:

$$\alpha(W)\to\alpha_1\to\alpha_2\to\cdots.$$

两种情况可能发生:

(1) M *停止*在 W 处,也就是说,序列在终止格局 α_r 处结束.

(2) M 在 W 处*没有停止*,也就是说,序列不会结束.

形式语法和 Turing 机

Turing 机可以用来识别语言. 具体地说,假设 M 是具有带符集合 A 的 Turing 机. 设 L 是 A 中的字符串 W 的集合,使得当 W 是输入时,M 停止在接受状态 s_Y. 我们将写 $L=L(M)$,并且我们说 M 识别形式语言 L. 因此如果 M 不停止在 W 处或 M 停止在 W 处但不在接受状态 s_Y 处,那么输入 W 不属于 $L(M)$.

下面的定理是本节的主要结果,它的证明超出本书的范围.

定理 13.7　形式语言 L 能被 Turing 机 M 识别,当且仅当 L 是一个类型 0 的形式语言.

注　三个停止状态的原因是 s_Y 和 s_N 被用来识别形式语言,而 s_H 被用作计算,这将在下一节中讨论.

例 13.14　假设一个具有带符集 $A=\{a,b,c\}$ 的 Turing 机 M 含有下面 4 个五元组:

$$q_1=s_0aas_0R,\ q_2=s_0bbs_0R,\ q_3=s_0BBs_NR,\ q_4=s_0ccs_YN.$$

(a) 假设 $W=W(a,b,c)$ 是一个不带 c 的输入.

根据五元组 q_1 和 q_2,M 处于状态 s_0,然后向右移动直到它遇到空白符 B. 然后将它的状态改变成不接受状态 s_N 并且停止下来.

(b) 假设 $W=W(a,b,c)$ 是一个至少带有一个 c 符号的输入.

根据五元组 q_4,当 M 最初遇到 W 中第一个 c 时,它会将它的状态转变成 s_Y 并且停止下来. 因此,M 识别由 a,b,c 构成并至少含有一个 c 的字符串 W 组成的形式语言 L. 也就是说,$L=L(M)$.

13.10　可计算的函数

可计算的函数定义于非负整数集合上. 有些教科书用 **N** 来表示这一集合. 我们用 **N** 来表示正整数集合,因而我们记

$$\mathbf{N}_0=\{0,1,2,3,\cdots\}.$$

在本节数字,整数和非负整数是同义的.

前一小节描述了 Turing 机 M 处理和识别字母资料的方式. 这里我们将说明 M 是怎样使用数字信息的. 首先,我们需要能通过带符集合 A 来表示,数字. 我们将以 1 作为带符号 a_1,并用 1^n 作为 $111\cdots1$,此处 1 连续出现 n 次.

定义 13.12　每个数字 n 将通过带表达 $\langle n\rangle$ 表示;此处 $\langle n\rangle=1^{n+1}$. 这样

$$\langle 4\rangle=11111=1^5,\ \langle 0\rangle=1,\ \langle 2\rangle=111=1^3.$$

定义 13.13　设 E 是一个表达. 那么 $[E]$ 将用来表示在 E 中 1 出现的次数. 因此,

$[11Bs_2a_3111Ba_4]=5$，$[a_4s_2Ba_2]=0$　和　$[\langle n\rangle]=n+1$.

定义 13.14　函数 $f:\mathbf{N}_0\to\mathbf{N}_0$ 是可计算的，如果存在一个 Turing 机 M 使得对每个整数 n，M 停止在 $\langle n\rangle$ 并且

$$f(n)=[\mathrm{term}(\alpha(\langle n\rangle))].$$

那么我们说 M 计算了 f.

也就是说，给一个函数 f 和一个整数 n，我们输入 $\langle n\rangle$ 和使用 M. 如果 M 总是停止在 $\langle n\rangle$ 处并且在最后格局里 1 的个数等于 $f(n)$，那么 f 是可计算的函数，我们说 M 计算 f.

例 13.15　函数 $f(n)=n+3$ 是可计算的. 输入是 $W=1^{n+1}$. 我们仅需在输入上再加两个 1，计算 f 的 Turing 机如下

$$M=\{q_1,q_2,q_3\}=\{s_011s_0L,\ s_0B1s_1L,\ s_1B1s_HN\}.$$

容易看出.

(1) q_1 使机器向左移动.

(2) q_2 在空格 B 上写下 1，并且使 M 向左移动.

(3) q_3 在空格 B 上写下 1，并且使 M 停止.

因此，对正整数 n，

$$s_01^{n+1}\to s_0B1^{n+1}\to s_1B1^{n+2}\to s_H1^{n+3}.$$

所以 M 计算 $f(n)=n+3$. 很明显，对任何正整数 k，函数 $f(n)=n+k$ 是可计算的.

定理 13.8　假设 $f:\mathbf{N}_0\to\mathbf{N}_0$ 和 $g:\mathbf{N}_0\to\mathbf{N}_0$ 是可计算的. 那么复合函数 $h=gof$ 也是可计算的.

我们给出这个定理的证明. 假设 M_f 和 M_g 是 Turing 机，它们分别计算 f 和 g. 给一个输入 $\langle n\rangle$，我们应用 M_f 到 $\langle n\rangle$，最后获得有 $[E]=f(n)$ 的表达 E. 然后我们安排 $E=s_01^{f(n)}$. 接下来在 E 上加上 1，获得 $E'=s_011^{f(n)}$ 并且应用 M_g 到 E'. 这将得到所需要的 E''，这里 $[E'']=g(f(n))=(gof)(n)$.

多元函数

本段中将定义一个可计算的 k 元函数 $f(n_1,n_2,\cdots,n_k)$. 首先我们需要用字母表 A 表示目录 $m=(n_1,n_2,\cdots,n_k)$.

定义 13.15　每一个 k 个整数的目录 $m=(n_1,n_2,\cdots,n_k)$ 由带表达 $\langle m\rangle$ 表示，这里

$$\langle m\rangle=\langle n_1\rangle B\langle n_2\rangle B\cdots B\langle n_k\rangle.$$

因此　　$\langle(2,0,4)\rangle=111B1B11111=1^3B1^1B1^5$.

定义 13.16　一个 k 元函数 $f(n_1,n_2,\cdots,n_k)$ 是可计算的，如果存在一个 Turing 机 M，使得对每一个目录 $m=(n_1,n_2\cdots,n_k)$，M 停止在 $\langle m\rangle$ 处，并且

$$f(m)=[\mathrm{term}(\alpha(\langle m\rangle))].$$

那么我们说 M 可计算 f.

本定义类似于一元的定义 13.14.

例 13.16　加函数 $f(m,n)=m+n$ 是可计算的. 输入是 $W=1^{m+1}B1^{n+1}$. 因此只需要去掉两个 1. 计算 f 的 Turing 机 M 如下

$$M=\{q_1,q_2,q_3,q_4\}=\{s_01Bs_1R,s_11Bs_HN,s_1BBs_2,s_21Bs_HN\}.$$

容易看出

(1) q_1 去掉第 1 个 1 并且将 M 向右移动.

(2) 如果 $m\neq0$，那么 q_2 去掉第二个 1，并且使 M 停止.

(3) 如果 $m\neq0$，q_3 将 M 向右移动经过空格 B.

(4) q_4 去掉并且使 M 停止.

因此，如果 $m\neq0$，我们有

$$s_0 1^{m+1}B1^{n+1}\to s_1 1^m B1^{n+1}\to s_H 1^{m-1}B1^{n+1}.$$

但是，若 $m=0$ 并且 $m+n=n$，我们有

$$s_0 1B1^{n+1}\to s_1 B1^{n-1}\to s_2 1^{n+1}\to s_H 1^n.$$

因此 M 计算 $f(m,n)=m+n$.

问题与解答

字符串

13.1 考虑字符串 $u=a^2ba^3b^2$ 和 $v=bab^2$. 找出：(a) uv；(b) vu；(c) v^2.

解 ☞ 写下第一个字符串的字母并将第二个字符串的字母紧跟其后.

(a) $uv=(a^2ba^3b^2)(bab^2)=a^2ba^3b^3ab^2$.

(b) $vu=(bab^2)(a^2ba^3b^2)=bab^2a^2ba^3b^2$.

(c) $v^2=vv=(bab^2)(bab^2)=bab^3ab^2$.

13.2 设 u 和 v 是问题 13.1 中的字符串，求 $|u|,|v|,|uv|,|vu|,|v^2|$.

解 ☞ 数每个字符串中字母个数得到

$$|u|=8,\ |v|=4,\ |uv|=12,\ |vu|=12,\ |v^2|=8.$$

13.3 假设 $u=a^2b$ 和 $v=b^3ab$. 求：(a) uvu；(b) $\lambda u, u\lambda, u\lambda v$.

解 ☞ (a) 写下 u 的字母，然后 v 的，最后 u 的字母得

$$uvu=a^2b^4aba^2b.$$

(b) 因为 λ 是空字符串，$\lambda u=u\lambda=u=a^2b$ 和 $u\lambda v=uv=a^2b^4ab$.

13.4 设 $w=abcd$. (a) 求 w 的所有子串. (b) 它们中的哪些是前缀?

解 ☞ (a) 子串是

$$\lambda, a, b, c, d, ab, bc, cd, abc, bcd, w=abcd.$$

我们强调 $v=acd$ 不是 w 的子串，即使它的所有字母都属于 w.

(b) 前缀是 $\lambda, a, ab, abc, w=abcd$.

13.5 对任何字符串 u 和 v，证明：(a) $|uv|=|u|+|v|$；(b) $|uv|=|vu|$.

证明 ☞ (a) 假设 $|u|=r$ 和 $|v|=s$，那么 uv 由 u 的 r 个字母后面跟着 v 的 s 个字母组成. 因此，

$$|uv|=r+s=|u|+|v|.$$

(b) 用(a)得 $|uv|=|u|+|v|=|v|+|u|=|vu|$.

13.6 假设 $|u|=n$. 求 u 的前缀的个数.

解 ☞ 比如 $u=a_1a_2\cdots a_n$. 那么有 $n+1$ 个前缀

$u_k=a_1a_2\cdots a_k$，其中 $k=1,2,\cdots,n$ 和 λ.

13.7 字母表 A 上的自由半群和自由幺半群的区别是什么?

解 ☞ A 上自由半群是在连接运算下所有非空字符串的集合，它不包括空串 λ. 另一方面，A 上自由幺半群包括空串 λ.

形式语言

13.8 设 $A=\{a,b\}$，用语言描述 A 上的下列形式语言(它们是 A^* 的子集).

(a) $L_1=\{(ab)^m: m>0\}$.

(b) $L_2=\{a^rba^sba^t: r,s,t\geqslant0\}$.

(c) $L_3=\{a^2b^ma^3: m>0\}$.

解 ☞ (a) L_1 由字符串 $w=ababab\cdots ab$ 组成，也就是说，以 a 开头与 b 交替出现并以 b 结尾.

(b) L_2 由所有恰好带有两个 b 的字符串组成.

(c) L_3 由所有以 a^2 开头，a^3 结尾，中间是一个或多个 b 的字符串组成.

13.9 设 $K=\{a,ab,a^2\}$ 和 $L=\{b^2,aba\}$ 是 $A=\{a,b\}$ 上的形式语言. 求：(a) KL；(b) LL.

解 ☞ (a) 将 K 上的字符串与 L 上的字符串连接，得

$$KL=\{ab^2,a^2ba,ab^3,ababa,a^2b^2,a^3ba\}.$$

(b) 将 L 上的字符串与 L 上的字符串连接，得

$$LL=\{b^4,b^2aba,abab^2,aba^2ba\}.$$

13.10 考虑 $A=\{a,b,c\}$ 上的形式语言 $L=\{ab,c\}$，求 (a) L^0；(b) L^3；(c) L^{-2}.

解 ☞ (a) 根据定义 $L^0=\{\lambda\}$.

(b) 用 L 中的字符串形成所有三个字符串序列

$$L^3=\{ababab,ababc,abcab,abc^2,cabab,cabc,c^2ab,c^3\}.$$

(c) 没有定义形式语言的负幂次方.

13.11 设 $A=\{a,b,c\}$. 求 L^*，这里 (a) $L=\{b^2\}$；(b) $L=\{a,b\}$；(c) $L=\{a,b,c^3\}$.

解 ☞ (a) L^* 由所有字符串 b^n 构成，此处 n 为偶数(包括空串 λ).

(b) L^* 由所有 a,b 构成的字符串组成.

(c) L^* 是由 A 中的那些字符串构成，这些字符串中完全由 c 构成的最大子串的长度是 3 的倍数.

13.12 考虑可数的字符集 $A=\{a_1,a_2,\cdots\}$. 设 L_k 为 A 上的那些下标之和为 k 的字符串 w 所形成的形式语言. 例如，$w=a_2a_3a_3a_6a_4\subset L_{18}$. (a) 求 L_4；(b) 证明 L_k 是有限的；(c) 证明 A^* 是可数的；(d) 证明 A 上的任何形式语言是可数的.

解 ☞ (a) L_4 中字符 a_n 中 n 不可能大于 4，L_4 中字符串不可能超过 4 个字符，因此我们有下面的列举

$$a_1a_1a_1a_1,\ a_1a_1a_2,\ a_1a_2a_1,\ a_2a_1a_1,\ a_1a_3,\ a_3a_1,\ a_2a_2,\ a_4.$$

(b) L_k 中只含有有限个字符 $a_1,a_2,\cdots,a_k$，L_k 中字符不可能超过 k 个，即 L_k 是有限的.

(c) A^* 是可数个有限集 L_k 的并，因此 A^* 也是可数的.

(d) L 是可数集合 A^* 的子集，因此 L 也是可数的.

正则表达，正则语言

13.13 设 $A=\{a,b,c\}$，对下面的每一个正则表达 r，描述语言 $L(r)$：

(a) $r=ab^*c^*$；(b) $r=a^*\vee b^*\vee c^*$

解 ☞ $L_{(r)}$ 由所有以 a,b,c 形式出现的字符串 w 组成使得

(a) w 恰含有一个 a 且 a 在开头，后跟 $n(\geqslant 0)$ 个 b，再跟 $m(\geqslant 0)$ 个 c.

(b) w 是仅以 a 或仅以 b 或仅以 c 构成的字符串，即

$$L(r)=\{\lambda,a,a^2,\cdots,b,b^2,\cdots,c,c^2,\cdots\}.$$

13.14 设 $A=\{a,b\}$，描述语言 $L(r)$，(a) $r=abb^*a$；(b) $r=b^*ab^*ab^*$；(c) $r=ab^*\wedge a^*$.

解 ☞ (a) $L(r)$ 由所有以 a 开头，以 a 结尾且中间包含一个或多个 b 所构成的字符串组成.

(b) $L(r)$ 由所有恰有两个 a 的字符串组成.

(c) 这里 r 不是一个正则表达，因为 $\wedge$ 不是一个形成正则表达的符号.

13.15 设 $A=\{a,b,c\}$ 和 $w=ac$. 说明 w 是否属于 $L(r)$，其中 (a) $r=ab^*c^*$；(b) $r=(a^*b\vee c)^*$.

解 ☞ (a) 是. 因为 $w=a\lambda c$ 且 $\lambda\in L(b^*)$，$c\in L(c^*)$.

(b) 否. 注意 $L(a^*b)$ 由字符串 a^nb 组成，因此如果 $L(r)$ 中含有字母 a，跟随 a 的只能是 a 或 b，而不能是 c.

13.16 设 $A=\{a,b,c\}$ 和 $w=abc$，说明 w 是否属于 $L(r)$，其中 (a) $r=a^*\vee(b\vee c)^*$；(b) $r=a^*(b\vee c)^*$.

解 ☞ (a) 否. $L(r)$ 由那些字符串构成，这些字符串是以 a 构成的或以 b,c 构成的.

(b) 是. 因为 $a \in L(a^*)$ 且 $bc \in <((b \vee c)^*)$.

13.17 令 $A=\{a,b\}$. 求一个正则表达 r 使 $L(r)$ 由所有字符串 w 组成,其中 (a) w 以 a^2 开头且以 b^2 结尾; (b) w 包含偶数个 a.

解 (a) 令 $r=a^2(a \vee b)^* b^2$.

(b) 注意, $s=b^* ab^* ab^*$ 由所有恰有两个 a 的字符串构成,因此设 $r=s^*=(b^* ab^* ab^*)^*$.

有限自动机,有限状态机

13.18 设 M 是有下面输入集 A, 状态集 S 和接受集 Y 的自动机.

$$A=\{a,b\},\ S=\{s_0,s_1,s_2\},\ Y=\{s_1\}.$$

假设 s_0 是 M 初始状态, M 的状态转移函数由图 13-10(a)给出.

(a) 画出 M 的状态图 $D=D(M)$.

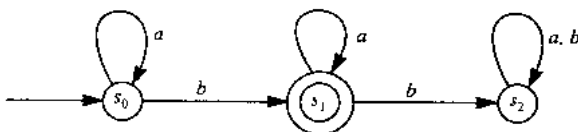
(b) 描述 M 接受的形式语言 $L=L(M)$.

解 (a) D 的状态图如图 13-10(b)所示. D 的结点是状态,双圈表示接受状态. 如果 $F(s_j,x)=s_k$, 就有 s_j 到 s_k 的标有输入符 x 的有向边. 同样,有一个特别的箭号指向初始状态 s_0.

(b) $L(M)$ 由所有含一个 b 的字符串 w 组成. 具体地说,如果输入字符 w 不含 b, 则在 s_0 结束;如果 w 含两个或两个以上 b 就在 s_2 结束. 否则 w 在仅有的接受状态 s_1 结束.

F	a	b
s_0	s_0	s_1
s_1	s_1	s_2
s_2	s_2	s_2

(a)



(b)

图 13-10

13.19 设 $A=\{a,b\}$. 构造一个能恰好接受 A 中含有偶数个 a 的字符串的自动机 M. 例如, *aababbab*, *aa*, *bbb*, *ababaa* 能被 M 接受,但 *ababa*, *aaa*, *bbabb* 不能被接受.

解 只需要两个状态 s_0 和 s_1. 假设 M 在某个步骤中处于 s_0 还是 s_1 是根据 a 出现的偶次数还是奇次数决定的. (因此 s_0 是接受状态,而 s_1 是拒绝状态.) 只有 a 将改变其状态. 同样, s_0 是初始状态. M 状态图如图 13-11 所示.

13.20 设 $A=\{a,b\}$. 构造一个自动机 M 使其能接受 A 中以 a 开头,且在 a 后面跟有 ≥ 0 个 b 的字符串.

解 见图 13-12.

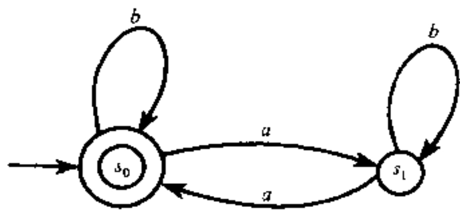


图 13-11

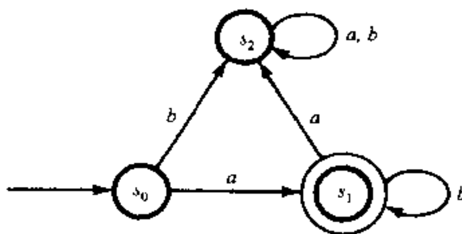


图 13-12

13.21 描述图 13-13 所示被自动机 M 接受的形式语言 L 的字符串 w.

解 仅当 w 中存在一个 b 跟随着 a 时系统才能到达接受状态 s_2.

13.22 描述图 13-14 所示被自动机 M 接受的形式语言 L 的字符串 w.

解 w 中每个 a 不能改变系统状态,而 w 中的每个 b 能从状态 s_i 到 s_{i+1}(mod4). 因此,如果 w 中 b 的个数 n 模 4 余 3, w 被 M 接受,即这里 $n=3,7,11,\cdots$.

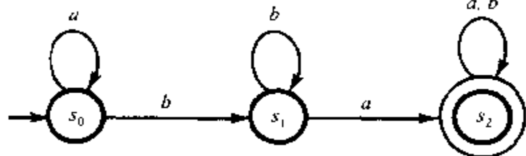


图 13-13

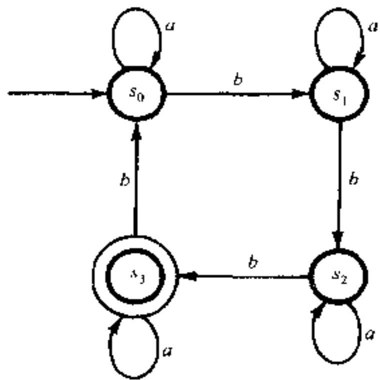


图 13-14

13.23 设 L 为 A 上的能被自动机 $M=\langle A,S,Y,s_0,F\rangle$ 接受的形式语言. 找出一个自动机 N 能接受 L^c，即 N 接受不属于 L 的 A 上的字符串.

解 ☞　简单互换 M 中接受状态与拒绝状态就得 N. 因此，w 被 N 接受当且仅当 w 被 M 拒绝. 正式地，$N=\langle A,S,S\backslash Y,s_0,F\rangle$.

13.24 设 $M=\langle A,S,Y,s_0,F\rangle$ 和 $M'=\langle A,S',Y',s_0',F'\rangle$ 是 A 上的两个自动机，它们接受的形式语言分别为 $L(M)$ 和 $L(M')$. 构造 A 上的能恰好接受 $L(M)\cap L(M')$ 的自动机 N.

解 ☞　设 $S\times S'$ 为 N 的状态集合. 设 (s,s') 是 N 的接受状态当且仅当 s 为 M 的接受状态和 s' 为 M' 的接受状态，(s_0,s_0') 为 N 的初始状态. N 的状态转移函数 $G:(S\times S')\times A\to(S\times S')$，定义为

$$G((s,s'),a)=(F(s,a),F'(s',a)).$$

那么 N 恰好接受 $L(M)\cap L(M')$ 中的字符串.

13.25 重述问题 13.24，现在设 N 恰好接受 $L(M)\cup L(M')$.

解 ☞　再设 $S\times S'$ 作为 N 的状态集合. 设 (s_0,s_0') 为 N 的初始状态，设 $(S\times Y')\cup(Y\times S')$ 为 N 的接受状态集，状态转移函数 G 定义为：

$$G((s,s'),a)=(F(s,a),F'(s',a)).$$

那么 N 恰好接受 $L(M)\cup L(M')$ 中的字符串.

13.26 设 M 为由图 13-15(a)所示的状态表格的有限状态机.

(a) 求输入字符集 A，状态集 S，输出集 Z 和初始状态.

(b) 画出 M 的状态图 $D=D(M)$.

(c) 假设 $w=aababaabbab$ 是一个输入字符串；求对应的输出字符串 v.

解 ☞　(a) 表格上方为输入符，左边为状态，表格中为输出符. 因此：

$$A=\{a,b\}\quad S=\{s_0,s_1,s_2,s_3\},\quad Z=\{x,y,z\}.$$

s_0 是初始状态，因为它是表格中第一个状态.

(b) 状态图 $D=D(M)$ 如图 13-15(b)所示，注意 D 的结点为 M 的状态.

假设

$$F(s_i,a_j)=(s_k,z_r),\quad \text{即}\quad f(s_i,a_j)=s_k\quad \text{和}\quad g(s_i,a_j)=z_r.$$

那么有由一对 a_j,z_r 标记的从 s_i 到 s_k 的有向边. 通常地，输入符 a_j 放在靠箭头的始端(靠近 s_i)而输出符 z_r 是放在箭头的中间.

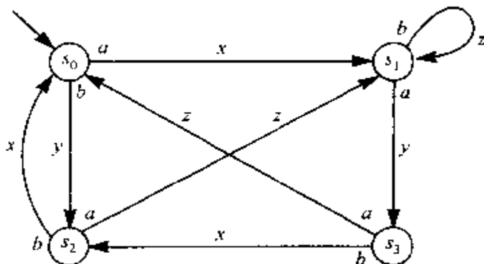
(c) 在初始状态开始时，我们通过被输入符标记的箭头从一个状态到另一状态，如下所示：

$$s_0\xrightarrow{a}s_1\xrightarrow{a}s_3\xrightarrow{b}s_2\xrightarrow{a}s_1\xrightarrow{b}s_1\xrightarrow{a}s_3\xrightarrow{a}s_0\xrightarrow{b}s_2\xrightarrow{b}s_0\xrightarrow{a}s_1\xrightarrow{b}s_1.$$

箭头上方的输出符产生了所需的输出字符串 $v=xyxzzyzyxxz$.

F	a	b
s_0	s_1, x	s_2, y
s_1	s_3, y	s_1, z
s_2	s_1, z	s_0, x
s_3	s_0, z	s_2, x

(a)



(b)

图 13－15

形式语法

13.27 定义（a）上下文无关的语法；（b）正则语法.

解 (a) 上下文无关的语法与型 2 的语法相同，即每个产生式都是 $A \to \beta$ 的形式，即左边是单个的变元，右边是一个或多个终结元或变元构成的字符串.

(b) 正则语法与型 3 语法相同，即每个产生式都是 $A \to a$ 或 $A \to aB$ 的形式，即左边是单个的变元，而右边是一个终结元或一个终结元跟一个变元.

13.28 求形式语法 G 生成的形式语言 $L(G)$，这里形式语法 G 是由变元 S, A, B，终结元 a, b 和产生式 $S \to aB, B \to b, B \to bA, A \to aB$ 构成的.

解 观察到第一个产生式只能用一次，这是因为起始符在其他地方不出现. 同样，我们只能通过最后使用第二个产生式得到终结元组成的字符串. 否则通过第三，第四个产生式交替增加 a 和 b. 换句话说，

$$L(G) = \{(ab)^n = ababab\cdots ab : n \in \mathbf{N}\}.$$

13.29 设 L 是所有由 a, b 构成的且 a 的个数为偶数的字符串集合，求一个生成 L 的形式语法 G. 我们声称带有以下产生式的形式语法 G 将生成 L：

$$S \to aA,\ S \to bB,\ B \to bB,\ B \to aA,\ A \to aB,\ A \to bA,\ A \to a,\ B \to b.$$

解 观察对于任何字符串 α，当产生式作用时，a 的个数与 A 的个数的和保持不变或增加 2. 因此任何以 a, b 形成的由 S 导出的字符串 w 必含有偶数个 a. 也就是 $L(G) \subseteq L$. 另一方面，哪些产生式应该用于 L 中的字符串 v 就非常明显了：即根据 v 以 a 或 b 开头用 $S \to aA$ 或 $S \to bB$；当其后的字母是一个 a 时用 $A \to aB$ 或 $B \to aA$，当其后的字母是个 b 时，用 $A \to bA$ 或 $B \to bB$；当对于 v 的最后一个字母用 $A \to a$ 或 $B \to b$. 因此 $L(G) = L$.

13.30 决定由下面产生式构成的形式语法 G 的类型：

(a) $S \to aA, A \to aAB, B \to b, A \to a$.

(b) $S \to aAB, AB \to bB, B \to b, A \to aB$.

(c) $S \to aAB, AB \to a, A \to b, B \to AB$.

(d) $S \to aB, B \to bA, B \to b, B \to a, A \to aB, A \to a$.

解 (a) 每个产生式都是形如 $A \to \alpha$，即左边是一个变元；因此 G 是上下文无关的或第 2 型形式语法.

(b) 每个产生式左边的长度不超过右边，所以 G 是第 1 型形式语法.

(c) 产生式 $AB \to a$ 意味着 G 是 0 型形式语法.

(d) G 是正则的或第 3 型形式语法，因为每个产生式都是形如 $A \to a$ 或 $A \to aB$.

13.31 设 L 是 $A = \{a, b\}$ 上的形式语言，它包含所有含一个 b 的字符串 w. 即

$$L = \{b, a^r b, ba^s, a^r ba^s : r > 0, s > 0\}.$$

(a) 求一个正则表达 r，使得 $L = L(r)$.

(b) 求一个产生形式语言 L 的正则语法 G.

解 (a) 设 $r = a^* ba^*$，那么 $L(r) = L$.

(b) 带有以下产生式的正则形式语法 G 生成 L

$$S \to (b, aA),\ A \to (b, aA, bB),\ B \to (a, aB).$$

即在任何由 S 导出的字符串中，字母 b 仅出现一次. G 是正则的，因为它有所需的形式.

13.32 设 L 是 $A=\{a,b,c\}$ 上的形式语言，由所有形如 $w=a^r b^s c^t$ 的字符串构成，这里 $r,s,t>0$. 即 a 后面跟着 b，b 后面跟着 c.

(a) 求一种正则表达 r，使 $L=L(r)$.

(b) 求一种产生形式语言 L 的正则语法 G.

解 (a) 设 $r=aa^*bb^*cc^*$，则 $L=L(r)$.

(b) 具有下面产生式的形式语法 G 生成 L

$$S\to aA,\ A\to(aA,bB),\ B\to(bB,c,cC),\ C\to(c,cC).$$

13.33 考虑带有下列产生式的正则语法 G

$$S\to aA,\ A\to aB,\ B\to bB,\ B\to a.$$

(a) 求字符串 $w=aaba$ 的导出树.

(b) 描述 G 生成的形式语言 L 中的所有字符串 w.

解 (a) 首先，注意到 S 导出 w 如下

$$S\Rightarrow aA\Rightarrow a(aB)\Rightarrow aa(bB)\Rightarrow aaba$$

图 13 - 16

图 13 - 16 表示了对应的导出树.

(b) 用产生式 1,2 和 r 次 3 式，再利用 4 得字符串 $w=aab^ra$，$r\geqslant0$，且没有其他的任何字符串能由 S 导出.

13.34 图 13 - 17 是上下文无关的形式语法 G 的形式语言 L 中的字符串 w 的导出树.

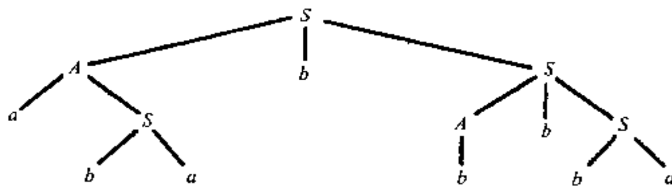


图 13 - 17

(a) 求 w；(b) 哪些终结元、变元和产生式一定在 G 中？

解 (a) 从左到右叶的序列产生字符串 $w=ababbbba$.

(b) 叶显示了 a 和 b 一定是终结元，内部结点显示 S 和 A 为变元且 S 为起始元. 每个变元的下代显示 $S\to AbS$，$A\to aS$，$S\to ba$、$A\to b$ 一定是产生式.

13.35 在形式语法 G 中，初始符 S 导出的字符串一定有生成树吗？

解 不是，只有型 2 和型 3 形式语法有导出树，即上下文无关的和正则语法.

13.36 以 Backus-Naur 形式重写 13.30 中每个形式语法 G.

解 Backus-Naur 形式仅适用于上下文无关的语法（它包含正则语法），因此仅有(a)和(d)能以 Backus-Naur 形式表达如下：

(i) 用 ::= 代替 →.

(ii) 把所有非终结元放入⟨ ⟩中.

(iii) 把所有左边相同的产生式由一个表达式写出来，这个表达式的右边是所有的产生式的右边的内容，中间用 | 隔开.

因此

(a) ⟨S⟩::=a⟨A⟩，⟨A⟩::=a⟨A⟩⟨B⟩|a，⟨B⟩::=b.

(d) ⟨S⟩::=a⟨B⟩，⟨B⟩::=b⟨A⟩|b|a，⟨A⟩::=a⟨B⟩|a.

Turing 机

13.37 设 M 是 Turing 机，决定下面情况对应的格局 α：

(a) M 在状态 s_3 且扫描带表达 $w=aabca$ 的第三个字母.

(b) M 在状态 s_2 且扫描带表达 $w=abca$ 的最后一个字母.

(c) 输入是带表达，$w=1^4B1^2$.

解 通过放状态符号正在扫描的带字母前面得到格局 α. 起始，M 在状态 s_0 且正在扫描输入的第一个字母. 因此，

(a) $\alpha=aas_3bca$；(b) $\alpha=abcs_2a$；(c) $\alpha=s_01111B11$.

13.38 假设 $\alpha=aas_2ba$ 为一个格局，且 Turing 机有下面的五元组 q，求 β 使得 $\alpha\rightarrow\beta$：

(a) $q=s_2bas_1L$；(b) $q=s_2bbs_3R$；(c) $q=s_2bas_2N$；(d) $q=s_3abs_1L$.

解 (a) 这里 M 擦去 b，写上 a，改变状态为 s_1，且向左移动，因此 $\beta=as_1aaa$.

(b) 这里 M 不改变已扫描的字母 b，改变状态到 s_3 且向右移动，因此 $\beta=aabs_3a$.

(c) 这里 M 擦去 b，写上 a，保持它的状态 s_2，没有移动，因此 $\beta=aas_2aa$.

(d) 这里 q 对 α 没有作用，因为 q 不是以 s_2b 开头.

13.39 设 $A=\{a,b\}$，$L=\{a^rb^s; r>0, s>0\}$. 即 L 由所有一个或多个 a 开头，后跟一个或多个 b 的字符串 w 组成. 求一个识辨 L 的 Turing 机 M.

解 策略是我们要 M (1)移向所有 a 的右边，(2)移向这个 b 的右边，(3)当它遇到空白符 B 时，停止在接受状态 s_Y 处. 这由下述五元组完成.

$$q_1=s_0aas_1R,\ q_2=s_1aas_1R,\ q_3=s_1bbs_2R,\ q_4=s_2bbs_2R,\ q_5=s_2BBs_YR.$$

具体地，q_1 和 q_2 做(1)，q_3 和 q_4 做(2)，q_5 做(3). 然而，我们也要 M 不接受输入字符串 w，当 w 不属于 L 时. 因此我们也需要下面的五元组

$$q_6=s_0BBs_NR,\ q_7=s_0bbs_NR,\ q_8=s_1BBs_NR,\ q_9=s_2aas_NR.$$

注意，当输入 $W=\lambda=B$ 时使用 q_6 空字符；当输入 W 是以 b 开头的表达时使用 q_7；当输入 W 只包含 a 时使用 q_8；当 W 仅包含字母 ba 时使用 q_9.

13.40 求一个 Turing 机 M，使它能识辨形式语言 $L=(ab)^*=\{(ab)^n; n\geqslant 0\}$.

解 给出输入 W，策略是使 M 擦去开头的 a，结尾的 b，开头的 a，结尾的 b，等等. 如果所有的字母均被擦去，那么 M 接受 W，因为 W 属于 L. 否则，我们要 M 不接受 W. 因此，M 将需要下面 7 个五元组：

(1) M 在初始状态 s_0，除去首位 a 且进入状态 s_1，或者如果 $W=\lambda$ 时 M 接受 W，或者如果 W 以 b 开头时，M 拒绝 W：

$$q_1=s_0aBs_1R,\ q_2=s_0BBs_YR,\ q_3=s_0bbs_NR.$$

(2) M 在状态 s_1 通过 a 向右移，直到 M 遇到 b 而进入状态 s_2，或者 M 拒绝 W，如果没有遇到 b：

$$q_4=s_1aas_1R,\ q_5=s_1bbs_2R,\ q_6=s_1BBs_NR.$$

(3) M 在状态 s_2 通过 b 向右移，直到 M 遇到 B 然后进入状态 s_3 向左移，或者 M 遇到 a 时拒绝 W：

$$q_7=s_2bbs_2R,\ q_8=s_2BBs_3L,\ q_9=s_2aas_NR.$$

(4) M 在状态 s_3 除去末尾的 b 进入状态 s_4 后向左移：

$$q_{10}=s_3bBs_4L.$$

(5) 在状态 s_4 的 M，如果遇到 B 则停止在状态 s_Y；或者向左移通过最右边的 b 进入状态 s_5：

$$q_{11}=s_4BBs_YL,\ q_{12}=s_4bbs_5L.$$

(6) 在状态 s_5 的 M 通过 b 向左移直到 M 遇到 a 或者遇到 B 而拒绝 W：

$$q_{13}=s_5bbs_5L,\ q_{14}=s_5aas_6L,\ q_{15}=s_5BBs_NL.$$

(7) 在状态 s_6 的 M 通过 a 向左移且遇到 B 时回到初始状态 s_0：

$$q_{16}=s_6aas_6L,\ q_{17}=s_6BBs_0R.$$

可计算的函数

13.41 求$\langle m\rangle$如果：(a) $m=5$；(b) $m=(4,0,3)$；(c) $m=(3,-2,5)$.

解 ☞ 回顾

$$\langle n\rangle = 1^{n+1} = 11^n$$

且 $\langle(n_1,n_2,\cdots n_r)\rangle=\langle n_1\rangle B\langle n_2\rangle B\cdots B\langle n_r\rangle$， 因此

(a) $\langle m\rangle=1^6=111111$.

(b) $\langle m\rangle=1^5B1^1B1^4=11111B1B1111$.

(c) $\langle m\rangle$对负整数没有定义.

13.42 根据下面的表达 E，求$[E]$：

(a) $E=a11s_2Bb111$.

(b) $E=aas_3bb$.

(c) $E=\langle m\rangle$ 其中 $m=(4,1,2)$.

(d) $E=\langle m\rangle$ 其中 $m=(n_1,n_2,\cdots,n_r)$.

解 ☞ 回顾$[E]$表示 E 中 1 的个数.因此：

(a) $[E]=5$.

(b) $[E]=0$.

(c) $[E]=10$.因为 $E=1^5B1^2B1^3$.

(d) $[E]=n_1+n_2+\cdots+n_r+r$,因为 n_k 产生的 1 的个数为 n_k+1.

13.43 设 f 为函数$\begin{cases}f(n)=n-1, & n>0,\\ 0, & n=0.\end{cases}$ 证明：f 是可计算的.

证明 ☞ 我们需要找出一个 Turing 机 M 来计算 f.具体地说，当 $n>0$ 时，我们要 M 除去输入$\langle n\rangle$中两个 1，当 $n=0$ 时，除去 1 个 1.当 $n>0$ 时，下面的五元组将完成这个任务.

$$q_1=s_01Bs_1R,\ q_2=s_1BBs_HN,\ q_3=s_11Bs_HN.$$

这里的 q_1 除去第一个 1，使 M 向右移，如果仅有 1 个 1，M 现正扫描一个空白符 B，且 q_2 叫计算机停止.否则，q_3 除去第 2 个 1，使 M 停止.

13.44 设 f 是函数 $f(x,y)=y$，证明 f 是可计算的.

解 ☞ 我们需要求一个 Turing 机 M 来计算 f，具体地说，我们要 M 除去$\langle x\rangle$中所有的 1 和$\langle y\rangle$中一个 1.下面的五元组将完成这个任务.

$$q_1=s_01Bs_0R,\ q_2=s_0BBs_1R,\ q_3=s_11Bs_HN.$$

这里 q_1 除去$\langle x\rangle$中所有的 1 当 M 向右移时.当 M 扫描空格 B 时，q_2 使 M 状态从 s_0 到 s_1 且使 M 向右移.然后 q_3 除去$\langle y\rangle$中第一个 1，且使 M 停止.

补 充 题

字符串

13.45 考虑字符串 $u=ab^2a^3$ 和 $v=aba^2b^2$，求

(a) uv；(b) vu；(c) u^2；(d) λu；(e) $v\lambda v$.

13.46 对于字符串 $u=ab^2a^3$ 和 $v=aba^2b^2$，求

$$|u|,|v|,|uv|,|vu|\text{和}|v^2|.$$

13.47 设 $w=abcde$，(a) 找出所有 w 的子串；(b) 哪些为前缀？

13.48 假设 $u=a_1a_2\cdots a_r$，且 a_k 为不同的.求 u 的所有子串的数目 n.

形式语言

13.49 设 $L=\{a^2,ab\}$，$K=\{a,ab,b^2\}$. 求：
(a) LK；(b) KL；(c) $L\vee K$；(d) $K\vee L$.

13.50 设 $L=\{a^2,ab\}$，求：(a) L^0；(b) L^2；(c) L^3.

13.51 设 $A=\{a,b,c\}$，描述 L^*. 若(a) $L=\{a^2\}$；(b) $L=\{a,b^2\}$；(c) $L=\{a,b^2,c^3\}$.

13.52 是否有 $(L^2)^*=(L^*)^2$？如果没有，那么它们有何种关系？

13.53 考虑一个可数的字母表 $A=\{a_1,a_2,\cdots\}$. 设形式语言 L_k 是 A 上由字符串 w 组成的，这些字符串 w 的字母下标的和等于 k.（参看问题 13.12）找出：(a) L_3；(b) L_5.

正则表达，正则语言

13.54 设 $A=\{a,b,c\}$. 对下面的正则表达 r 描述形式语言 $L(r)$
(a) $r=ab^*c$；(b) $r=(ab\vee c)^*$；(c) $r=ab\vee c^*$.

13.55 设 $A=\{a,b\}$，找出一个正则表达 r 使得 $L(r)$ 是由字符串 w 所构成.
(a) w 恰好含 3 个 a.
(b) a 的数目能被 3 整除.
(c) w 以 b 开头并以 b 结尾. 且 bab 不是 w 的子串；即不管 a 出现在 w 中的何处，它的指数不小于 2.

13.56 设 $A=\{a,b,c\}$，$w=ac$. 对于(a) $r=a^*bc^*$；(b) $r=a^*b^*c$；(c) $r=(ab\vee c)^*$，说明 w 是否属于 $L(r)$.

13.57 设 $A=\{a,b,c\}$，$w=abc$. 设(a) $r=ab^*(bc)^*$；(b) $r=a^*\vee(b\vee c)^*$；(c) $a^*b(bc\vee c^2)^*$，说明 w 是否属于 $L(r)$.

有限自动机

13.58 设 $A=\{a,b\}$，构造一个自动机 M 使得 $L(M)$ 将由 b 的个数能被 3 整除的字符串所组成.
（提示：需要三种状态）

13.59 设 $A=\{a,b\}$. 构造一个自动机 M 使得 $L(M)$ 是由以 a 开头且以 b 结尾的字符串 w 构成.

13.60 设 $A=\{a,b\}$. 构造自动机 M 来接受形式语言 $L(M)=\{a^rb^s: r>0, s>0\}$.

13.61 设 $A=\{a,b\}$. 构造自动机 M 来接受形式语言 $L(M)=\{b^rab^s: r>0, s>0\}$.

13.62 设 $A=\{a,b\}$. 构造自动机 M 使得 $L(M)$ 是由 a 的个数被 2 整除且 b 的个数被 3 整除的字符串构成.
（提示：利用问题 13.9，13.58 和 13.24）

13.63 求形式语言 $L(M)$，它被图 13-18 中的自动机 M 接受.

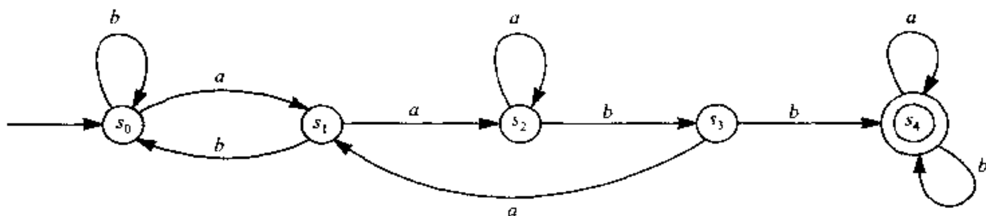


图 13-18

有限状态机

13.64 设 M 是具有图 13-19 的状态表的有限状态机.
(a) 求输入集合 A，状态集合 S，输出集合 Z 和 M 的初始状态.
(b) 画出 M 的状态图 $D=D(M)$.
(c) 若输入是字符串 $w=a^2b^2ab^2a^2b$，求输出字符串 v.

13.65 设 M 是有限状态机，具有输入集合 $A=\{a,b,c\}$，输出集合 $Z=\{x,y,z\}$ 和图13-20中的状态图 $D=D(M)$. (a) 构造 M 的状态表. (b) 若输入是字符串 $w=ca^2b^2ac^2ab$，求输出字符串 v.

F	a	b
s_0	s_2,y	s_1,z
s_1	s_2,x	s_3,y
s_2	s_2,y	s_1,z
s_3	s_2,z	s_0,x

图 13 - 19

图 13 - 20

13.66　对图 13 - 21 中的每个自动机，具有输入集合 $A=\{a,b\}$，输出集合 $Z=\{x,y,z\}$. 求输出字符串 v，若输入是字符串 $w=aba^2b^2ab^2a^2ba^2$.

(a)

(b)

图 13 - 21

形式语法

13.67　决定形式语法 G 的类型，G 是由下列产生式构成的：

(a) $S\to aAB$; $S\to AB$; $A\to a$; $B\to b$.

(b) $S\to aB$; $B\to AB$; $aA\to b$; $A\to a$; $B\to b$.

(c) $S\to aB$; $B\to bB$; $B\to bA$; $A\to a$; $B\to b$.

13.68　求生成形式语言 L 的正则语法 G，这里 L 是由所有 a，b 组成的且没有连续的两个 a 的字符串组成.

13.69　求生成形式语言 L 的上下文无关的形式语法 G，这里 L 是由所有的 a 和 b 组成的，且 a 的个数是 b 的两倍的字符串组成.

13.70　求生成形式语言 L 的形式语法 G，这里 L 是由所有形同 $a^nba^n(n\geqslant 0)$ 的字符串构成的.

13.71　说明问题 13.70 中的形式语法 G 不是正则的.

(提示：利用 Pumping 引理.)

13.72　描述形式语言 $L=L(G)$，这里 G 有产生式：

$S\to aA$, $A\to bbA$, $A\to C$.

13.73　描述形式语言 $L=L(G)$，这里 G 有产生式：

$S\to aSb$, $Sb\to bA$, $abA\to C$.

13.74　用 Backus-Naur 的形式写出问题 13.67 中的每个形式语法 G.

13.75　设 G 是上下文无关的形式语法且有产生式 $S\to(a,aAS)$ 和 $A\to bS$.

(a) 以 Backus-Naur 的形式写出 G.

(b) 求字符串 $w=abaabaa$ 的导出树.

13.76　图 13 - 22 是上下文无关的形式语法 G 的形式语言 L 中的一个字符串 w 的导出树.

图 13 - 22

(a) 求 w; (b) 哪些终结元、变元、产生式一定属于 G?

Turing 机

13.77 设 M 是一个 Turing 机. 决定下列每种情况对应的格局 α.

(a) M 在状态 s_2 中,正在扫描带表达 $u=abbaa$ 中的第三个字母.

(b) M 在状态 s_3 中,正在扫描带表达 $w=aabb$ 中的最后一个字母.

(c) 输入是字符串 $W=a^3b^3$.

(d) 输入是带表达 $W=\langle(3,2)\rangle$.

13.78 假设 $\alpha=abs_2aa$ 是一个格局. 求 β,使得 $\alpha\rightarrow\beta$,假设 Turing 机 M 有下列的五元组 q:

(a) $q=s_2abs_1R$. (b) $q=s_2aas_3L$. (c) $q=s_2abs_2N$.

(d) $q=s_2abs_3L$. (e) $q=s_3abs_2R$. (f) $q=s_2aas_2N$.

13.79 对于格局 $\alpha=s_2aBab$ 重复问题 13.78.

13.80 求不同的格局 α 和 β 和 Turing 机 M,使得序列 $\alpha\rightarrow\beta\rightarrow\alpha\rightarrow\beta\rightarrow\cdots$ 没有终止.

13.81 假设 $\alpha\rightarrow\beta_1$ 和 $\alpha\rightarrow\beta_2$,是否一定有 $\beta_1=\beta_2$?

13.82 假设 $\alpha=\alpha(W)$ 对某个输入 W,并假设 $\alpha\rightarrow\beta\rightarrow\alpha$. M 能识辨 W 吗?

13.83 设 $A=\{a,b\}$,求一个 Turing 机 M,来识辨形式语言 $L=\{ab^n:n>0\}$,即 L 由所有以一个 a 开头接下来是一个或多个 b 的字符串 W 构成.

13.84 设 $A=\{a,b\}$. 求一个 Turing 机 M 来识辨有限形式语言 $L=\{a,a^2\}$,即 L 是由 a 的非零次幂的前两个构成.

可计算的函数

13.85 求 $\langle m\rangle$. 若:(a) $m=6$; (b) $m=(5,0,3,1)$; (c) $m=(0,0,0)$; (d) $m=(2,3,-1)$.

13.86 对于下列表达求 $[E]$:(a) $E=111s_2aa1B111$; (b) $E=a11bs_1Bb$; (c) $E=\langle m\rangle,m=(2,5,4)$.

13.87 设 f 是函数 $f(n)=\begin{cases}n-2, n>1,\\ 0, n=0 \text{ 或 } n=1\end{cases}$. 说明 f 是可计算的.

13.88 设 f 是函数 $f(x,y)=x$. 说明 f 是可计算的.

补充题答案

13.45 (a) $uv=ab^2a^4ba^2b^2$; (b) $uv=aba^2b^2ab^2a^3$; (c) $u^2=ab^2a^4b^2a^3$; (d) $\lambda u=u=ab^2a^3$; (e) $v\lambda v=v^2=aba^2b^2aba^2b^2$.

13.46 $|u|=6$; $|v|=6$; $|uv|=|vu|=12$; $|v^2|=12$.

13.47 (a) $\lambda,a,b,c,d,e,ab,bc,cd,de,abc,bcd,cde,abcd,bcde,w=abcde$.

(b) $\lambda,a,ab,abc,abcd,w=abcde$.

13.48 若 $u\neq\lambda$,那么 $n=1+[r+(r-1)+\cdots+2+1]=1+r(r+1)/2$. 若 $u=\lambda$,那么 $n=1$.

13.49 (a) $LK=\{a^3,a^3b,a^2b^2,aba,abab,ab^3\}$.

(b) $KL=\{a^3,a^2b,aba^2,abab,b^2a^2,b^2ab\}$.

(c) $L\vee K=\{a^2,ab,a,ab,b^2\}$.

(d) $K\wedge L$ 没有定义.

13.50 (a) $L^0=\{\lambda\}$.

(b) $L^2=\{a^4,a^3b,aba^2,abab\}$.

(c) $L^3=\{a^6,a^5b,a^3ba^2,a^3bab,aba^4,aba^3b,ababa^2,ababab\}$.

13.51 (a) $L^*=\{a^n;n$ 是偶数$\}$.

(b) 所有由 a 和 b 的偶数幂构成的字符串.

(c) a,b,c 构成那些字符串,b 的幂是偶数,c 的幂是 3 的倍数.

13.52 否. $(L^2)^*\subseteq(L^*)^2$.

13.53 (a) $a_1a_1a_1,a_1a_2,a_2a_1,a_3$.

(b) $a_1a_1a_1a_1a_1, a_1a_1a_1a_2, a_1a_1a_2a_1, a_1a_2a_1a_1, a_2a_1a_1a_1, a_1a_1a_3, a_1a_3a_1, a_3a_1a_1, a_2a_3, a_3a_2, a_1a_4, a_4a_1, a_5$.

13.54 (a) $L(r)=\{ab^nc: n\geqslant 0\}$.

(b) 所有由 x 和 c 构成的字符串,这里 $x=ab$.

(c) $L(r)=ab\cup\{c^n: n\geqslant 0\}$.

13.55 (a) $r=b^*ab^*ab^*ab^*$; (b) $r=(b^*ab^*ab^*ab^*)^*$; (c) $r=bb^*a(a\vee b)^*ab^*b$.

13.56 (a) 否; (b) 是; (c) 否.

13.57 (a) 是; (b) 否; (c) 否.

13.58 见图 13-23.

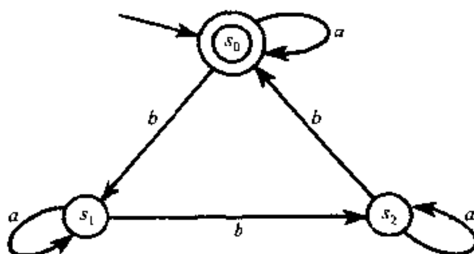


图 13-23

13.59 见图 13-24.

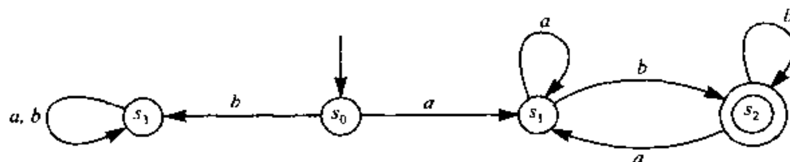


图 13-24

13.60 见图 13-25.

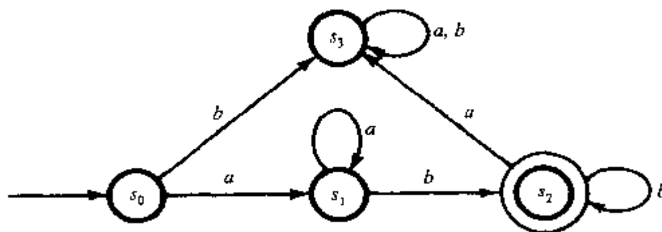


图 13-25

13.61 见图 13-26.

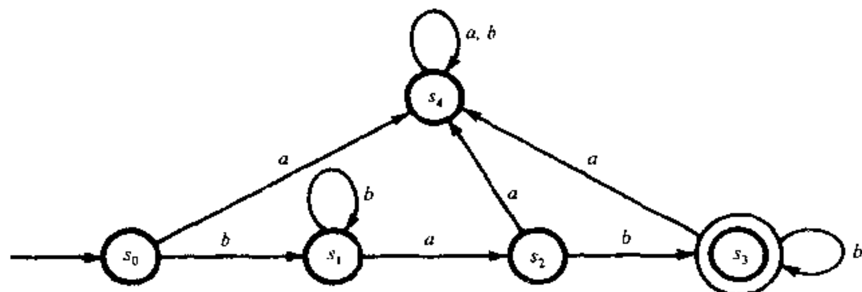


图 13-26

13.62　见图 13 - 27.

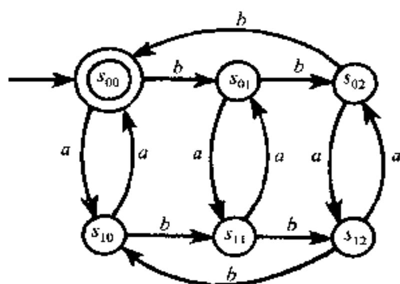


图 13 - 27

13.63　$L(M)$由所有含有 $aabb$ 作为子串的字符串 w 构成.

13.64　(a) $A=(a,b)$, $S=\{s_0, s_1, s_2, s_3\}$, $Z=\{x,y,z\}$, s_0 是初始状态.

(b) 见图 13 - 28.

(c) $v=y^2zyzxzxyz$.

13.65　(a) 见图 13 - 29. (b) $v=xy^2xz^3xyx$.

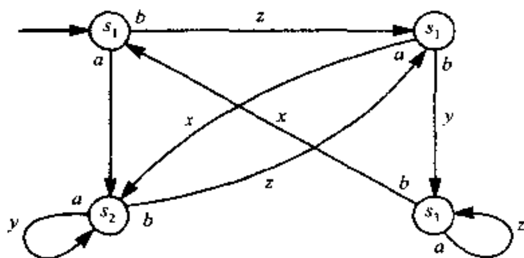


图 13 - 28

F	a	b	c
s_0	s_1, x	s_2, z	s_1, x
s_1	s_1, y	s_2, z	s_0, z
s_0	s_1, z	s_2, x	s_0, x

图 13 - 29

13.66　(a) $v=xyzxy^2z^2x^2z^2y^2$; (b) $v=zyxy^2zx^2zxy^2xy$.

13.67　(a) 2 型; (b) 0 型; (c) 3 型.

13.68　$S\to(a,b,aB,bA)$, $A\to(bA,ab,a,b)$, $B\to(b,bA)$.

13.69　$S\to(AAB,ABA,BAA)$, $A\to(a,BAAA,ABAA,AABA,AAAB)$,

$B\to(b,BBAA,BABA,aBAAB,ABAB,AABB)$.

13.70　$S\to(aSa,b)$.

13.72　$L=\{ab^{2n}c : n\geqslant 0\}$.

13.73　$L=\{a^ncb^n : n>0\}$.

13.74　(a) $\langle S\rangle ::= a\langle A\rangle\langle B\rangle \mid \langle A\rangle\langle B\rangle$, $\langle A\rangle ::= a$, $\langle B\rangle ::= b$.

(b) 对 0 型形式语言没有定义.

(c) $\langle S\rangle ::= a\langle B\rangle$, $\langle B\rangle ::= b\langle B\rangle \mid b\langle A\rangle$, $\langle A\rangle ::= a\mid b$.

13.75　(a) $\langle S\rangle ::= a\mid a\langle A\rangle\langle S\rangle$, $\langle A\rangle ::= b\langle S\rangle$; (b) 见图 13 - 30.

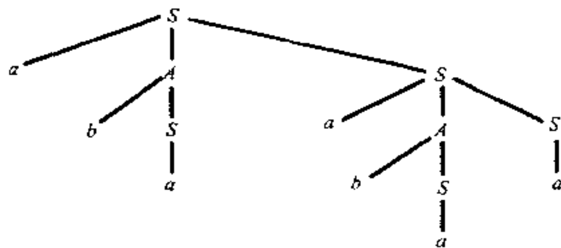


图 13 - 30

13.76　(a) $w=aababa$; (b) $S\to aAB$, $A\to aB$, $B\to ba$.

13.77　(a) $\alpha=abs_2baa$; (b) $\alpha=aabs_3b$; (c) $\alpha=s_0aaabbb$; (d) $\alpha=s_01111B111$.

13.78 (a) $\beta=abbs_1a$; (b) $\beta=as_3baa$; (c) $\beta=abs_2ba$; (d) $\beta=as_3bba$; (e) q 对 α 没有作用;
(f) $\beta=\alpha=abs_2aa$.

13.79 (a) $\beta=bs_1Bab$; (b) $\beta=s_2BaBab$; (c) $\beta=s_2bBab$; (d) $\beta=s_3BbBab$; (e) q 对 α 没有作用;
(f) $\beta=\alpha=s_2aBab$.

13.80 $\alpha=s_0a$; $\beta=s_1b$, $q_1=s_0abs_1N$; $q_2=s_1Bas_0N$.

13.81 是.

13.82 否,因为 $\alpha\to\beta\to\alpha\to\beta\to\cdots$ 没有止境.

13.83 $q_1=s_0BBs_NR$(否);$q_2=s_0bbs_NR$(否);
$q_3=s_0aas_1R$;$q_4=s_1BBs_NR$(否);
$q_5=s_1aas_NR$(否);$q_6=s_1bbs_2R$; $q_7=s_2bbs_2R$(否);
$q_8=s_2aas_NR$(否);$q_9=s_2BBs_YR$(是).

13.84 $q_1=s_0BBs_NR$(否);$q_2=s_0bbs_NR$(否);
$q_3=s_0aas_1R$;$q_4=s_1BBs_YR$(接受);
$q_5=s_1bbs_NR$(否); $q_6=s_1aas_2R$;
$q_7=s_2BBs_YR$(是);$q_8=s_2aas_NR$(否);
$q_9=s_2bbs_NN$(否).

13.85 (a) $\langle 6\rangle=1^7$; (b) $\langle m\rangle=1^6B1B1^4B1^2$; (c) $\langle m\rangle=1B1B1$; (d) 没有定义.

13.86 (a) $[E]=7$; (b) $[E]=2$; (c) $[E]=14$.

13.87 策略:去掉前三个 1.
$q_1=s_01Bs_1R$, $q_2=s_1BBs_HN$(停止), $q_3=s_11Bs_2R$,
$q_4=s_2BBs_HN$(停止), $q_5=s_21Bs_HN$.

13.88 策略:去掉第一个 1 及 B 后面的所有 1.
$q_1=s_01Bs_1R$, $q_2=s_111s_1R$, $q_3=s_1BBs_2R$,
$q_4=s_21Bs_3R$, $q_5=s_31Bs_3R$, $q_6=s_3BBs_HN$(停止).

第十四章　有序集与格

14.1　引　言

顺序和先后关系经常在数学和计算机科学中出现.本章将使这些概念精确化.在此,我们也定义一种格,它是一种特别的有序集.

14.2　有序集

假设 R 是集合 S 的一种关系,它满足下面三个性质:

[$\mathbf{O}_1$](反身性)　对任何 $a\in S$,有 aRa.

[$\mathbf{O}_2$](反对称性)　若 aRb 且 bRa,则 $a=b$.

[$\mathbf{O}_3$](传递性)　若 aRb 且 bRc,则 aRc.

则称 R 为一个*偏序*或简称一个*序关系*.带有偏序关系 R 的集合 S 叫做一个*偏序集*,或简称为*有序集*.当我们要标明 R 时,记作 (S,R).

最熟悉的序关系叫常序,比如,或更广泛地,在实数 $\mathbf{R}$ 的子集中正整数 $\mathbf{N}$ 中的"$\leqslant$"关系(读作小于等于)。由于这个原因,一个偏序关系通常记作$\precsim$;即

$$a\precsim b.$$

读作"a 先于 b".类似地,

$a\prec b$ 意为 $a\precsim b$ 且 $a\neq b$;读作"a 严格先于 b".

$b\succsim a$ 意为 $a\precsim b$;读作"b 后于 a".

$b\succ a$ 意为 $a\prec b$;读作"b 严格后于 a".

$\not\precsim$,$\not\prec$,$\not\succsim$和$\not\succ$的定义是自然的.当不产生混淆时,常用符号$\leqslant$,$<$,$>$和$\geqslant$分别代替符号$\precsim$,$\prec$,$\succ$和$\succsim$.

例 14.1　(a) 设 S 为任意的一个集簇,集合包含关系$\subseteq$是 S 的一个偏序关系.特别地,对任意集合 A 有 $A\subseteq A$;若 $A\subseteq B$ 且 $B\subseteq A$,则 $A=B$;若 $A\subseteq B$ 且 $B\subseteq C$,则 $A\subseteq C$.

(b) 设 $\mathbf{N}$ 为正整数集合.a 整除 b,记作"$a|b$".例如,$2|4$,$3|12$,$7|21$,等等.这种整除关系是 $\mathbf{N}$ 上的一个偏序关系.

(c) 整除关系"$|$"不是整数集 $\mathbf{Z}$ 上的偏序关系.特别地,整除在 $\mathbf{Z}$ 上的关系不是反对称的.例如,$2|-2$ 和 $-2|2$,但 $2\neq-2$.

(d) 设整数集合 $\mathbf{Z}$.定义 aRb,当且仅当存在一个正整数 r 使得 $b=a^r$.例如,$2R8$ 因为 $8=2^3$,因此 R 是 $\mathbf{Z}$ 上的偏序关系.

对偶序

设$\precsim$为集合 S 的任何偏序.关系$\succsim$,即 a 后于 b,也是 S 的偏序,叫做*对偶序*.显然 $a\precsim b$ 当且仅当 $b\succsim a$;因此对偶序$\succsim$是$\precsim$的逆,即$\succsim=\precsim^{-1}$.

有序子集

设 A 为有序集 S 的一个子集,假设 $a,b\in A$.在 A 中定义 $a\precsim b$ 当且仅当在 S 中有 $a\precsim b$.A 的这个偏序叫 A 上的*诱导序*,带有诱导序的子集 A 被称为 S 的*有序子集*.除非特殊说明,序集 S 的任何子集被认为是 S 的有序子集.

半序

假定$\prec$是集合 S 上的一种关系,满足下面两个性质:

[Q_1]（非反身性） 对任何 $a\in A$，有 $a\nprec a$.

[Q_2]（传递性） 若 $a\prec b$ 且 $b\prec c$，则 $a\prec c$.

那么 $\prec$ 叫作 S 的半序.

偏序和半序有着紧密联系. 特别地，如果 $\precsim$ 是集合 S 上的偏序，则 $a\prec b$ 意为 $a\precsim b$ 且 $a\neq b$，即 $\prec$ 是 S 上的半序. 相反地，如果 $\prec$ 是 S 上的半序，则 $a\precsim b$ 意为 $a\prec b$ 或 $a=b$，即 $\precsim$ 是 S 上的偏序. 这就允许我们在偏序和与其相应的半序中选择较方便的一个.

可比较性，线性序集

假设 a 和 b 是偏序集合 S 的元素. 我们说 a 和 b 是*可比较的*，如果有

$$a\precsim b \text{ 或 } b\precsim a.$$

即一个先于另一个. 否则 a 和 b 是*不可比较的*，记作

$$a \parallel b,$$

即既没有 $a\precsim b$ 也没有 $b\precsim a$.

"偏"是用来定义偏序集 S，因为 S 的某些元素是不需要可比较的. 换句话说，假设 S 的每一对元素都是可比较的，则 S 被称为*全序或者线性序*，且 S 被叫做一条*链*. 尽管序集 S 可能不是线性序集，S 的子集 A 仍有可能是线性序集. 很明显，线性序集 S 的每一个子集一定是线性序.

例 14.2 (a) 考虑正整数集合 $\mathbf{N}$ 在整除下的序关系. 21 和 7 可比较，因为 $7|21$. 但是 3 和 5 不可比较的，因为既没有 $3|5$ 也没有 $5|3$. 因此 $\mathbf{N}$ 在整除下的序关系不是线性序集. $A=\{2,6,12,36\}$ 是 $\mathbf{N}$ 的一个线性序子集，因为 $2|6$，$6|12$ 和 $12|36$.

(b) 带有常序 $\leqslant$ 的正整数集 $\mathbf{N}$ 是线性序集，故 $\mathbf{N}$ 的每个有序子集都是线性序集.

(c) 含有两个或多个元素的集合 A 的幂集 $P(A)$ 在集合包含关系下不是线性序集. 例如，假设 a 和 b 属于 A，那么 $\{a\}$ 与 $\{b\}$ 是不可比较的. 观察空集 $\varnothing$，$\{a\}$ 和 A 形成 $P(A)$ 的线性有序子集，因为 $\varnothing\subseteq\{a\}\subseteq A$. 类似地，$\varnothing$，$\{b\}$ 和 A 也形成 $P(A)$ 的线性有序子集.

积集和积序

有很多方法定义所给有序集的笛卡儿积上的序关系. 下面是其中的两个方法：

(a) **积序** 设 S 和 T 是有序集，那么下面是积集 $S\times T$ 上的一种序关系，称为*积序*

$$(a,b)\precsim(a',b')\text{，如果 } a\leqslant a' \text{ 和 } b\leqslant b'.$$

(b) **字典排序** 设 S 和 T 是线性序集，那么下面是积集 $S\times T$ 上的一种序关系，称为*字典排序*或*字典序*.

$$(a,b)\precsim(a',b')\text{，如果 } a\prec a' \text{ 或如果 } a=a' \text{ 且 } b\prec b'.$$

这个序能推广到 $S_1\times S_2\times\cdots\times S_n$ 上：

$$(a_1,a_2,\cdots,a_n)\prec(a'_1,a'_2,\cdots,a'_n)\text{，若对于 } i=1,2,\cdots,k-1.$$

有 $a_i=a'_i$ 且 $a_k\prec a'_k$.

注 字典排序也是线性的.

Kleene 闭包与序

设 A(非空)是一个线性序字母表. 回顾 A^*，称作 A 的 Kleene 闭包，由 A 中所有字符串 w 构成，$|w|$ 表示 w 的长度. 因此下面是 A^* 上的两个序关系.

(a) **字母排序** 读者肯定熟悉 A^* 的字母顺序. 即

(i) $\lambda\prec w$，λ 是空字符串，w 是任何非空字符串.

(ii) 设 $u=au'$ 和 $v=bv'$ 是不同的非空字符串，$a,b\in A$，$u',v'\in A^*$，那么

$$u\prec v\text{，如果 } a\prec b \text{ 或如果 } a=b \text{ 但 } u'\prec v'$$

(b)**长度-字母序**　这里 A^* 先按长度排,再按字母顺序排.即对 A^* 中任何不同字符串 u,v,
$u<v$,如果 $|u|<|v|$ 或如果 $|u|=|v|$ 但按字母顺序 u 先于 v.

例如,"*to*"先于"*and*"因为 $|to|=2$ 但 $|and|=3$,然而,"*an*"先于"*to*"因为它们有相同的长度,但按字母顺序"*an*"先于"*to*".这个序也称作自由半群序.

14.3　偏序集的 Hasse 图

设 S 是一个偏序集,且 a,b 属于 S.我们说 a 是 b 的一个直接前元或 b 是 a 的一个直接继元,或者 b 盖住 a,记作

$$a \ll b.$$

如果 $a<b$,在 S 中没有元素介于 a 与 b 之间,即不存在 $c\in S$,使得 $a<c<b$.

假定 S 是有限偏序集.S 中的序将完全清楚,如果我们知道 S 中所有 $a\ll b$ 的元素对 a,b.则知道 S 上的≪关系.这是因为 $x<y$ 当且仅当 $x\ll y$ 或在 S 中存在元素 $a_1,a_2,\cdots,a_m$ 使得

$$x\ll a_1\ll a_2\ll\cdots\ll a_m\ll y.$$

有限偏序集 S 的 Hasse 图是直接图解,它的顶点是 S 的元素,从 a 到 b 有一个有向边,当 $a\ll b$ 时.(我们不画一个从 a 指向 b 的箭头,而是将 b 置于高于 a 的地方,然后画一线将它们连起来.很清楚,向上运动引起后元.)因此在图中,从点 x 到点 y 有一有向路,当且仅当 $x<y$.同样,在 S 的图中没有环,因为序关系是反对称的.

偏序集 S 的 Hasse 图对描述 S 中元素的类型很有用.有时我们利用给出其 Hasse 图来定义一个偏序集.注意偏序集 S 的 Hasse 图不需要连通.

注　有限偏序集 S 的 Hasse 图在 9.9 节中作为有向无圈图(DAG)已出现过.这里的内容不依赖于以前的内容.这里我们主要把序看成"小于"或"大于"的关系,而不是有向连接关系.因此,在内容中有一些重复.

例 14.3　(a) 设 $A=\{1,2,3,4,6,8,9,12,18,24\}$ 是在"x 整除 y"关系下的序集.A 的 Hasse 图由图 14-1(a)中给出.(与有根树不同,在偏序集的 Hasse 图中,线的方向总是向上.)

(b) 设 $B=\{a,b,c,d,e\}$.图 14-1(b)中的 Hasse 图,用自然方式定义 B 中偏序.即 $d\leqslant b,d\leqslant a,e\leqslant c$,等等.

(c) 有限线性序集的 Hasse 图,即一个有限链,即由一条路构成.例如,图 14-1(c)表示五个元素的链的 Hasse 图.

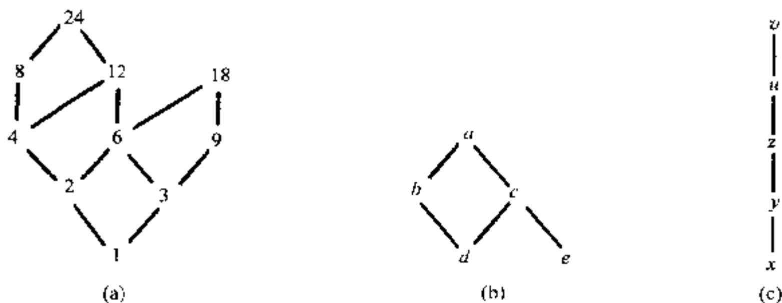


图 14-1

例 14.4　正整数 m 的一个划分是一个和为 m 的正整数的集合.例如,$m=5$ 的七个划分如下

5,3—2,2—2—1,1—1—1—1—1,
4—1,3—1—1,2—1—1—1

我们给整数 m 的划分定序如下:A 的划分 P_1 先于划分 P_2,如果 P_1 中整数加起来得到 P_2 中的整数,或进一步划分 P_2 中整数得到 P_1 中的整数.

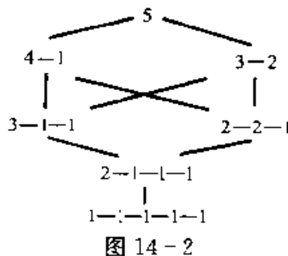


图 14-2

例如，

$$2-2-1 \text{ 先于 } 3-2,$$

因为 $2+1=3$，另一方面，$3-1-1$ 与 $2-2-1$ 是不可比较的.

图 14－2 给出了 $m=5$ 划分的 Hasse 图.

极小元素和极大元素，最小元素和最大元素

设 S 为一个偏序集. S 中的一个元素 a 叫做*极小元素*，如果 S 中没有其他元素严格先于 a. 类似地，S 中的一个元素 b 叫做*极大元素*，如果 S 中没有元素严格后于 b（比 b 大）. 注意，S 可以有多于一个极小元素和极大元素.

如果 S 是无限的，那么 S 可能没有极小和极大元素. 例如，带有常序 $\leqslant$ 的整数集合 **Z** 没有极小和极大元素. 换句话说，如果 S 是有限的，那么 S 一定至少有一个极小元素和一个极大元素.

S 中的一个元素 a 叫做*最小元素*，如果对于 S 中每一个元素 x 有

$$a \lesssim x,$$

即 a 先于 S 中其他每一个元素. 类似地，S 中的一个元素 b 叫做*最大元素*，如果对于 S 中每一个元素 y 有

$$y \lesssim b,$$

即如果 b 后于 S 中其他每一个元素. 注意，S 至多有一个最小元素，它一定是极小元素；S 中至多有一个最大元素，它一定是极大元素. 总的说来，S 可能既无最小元素也无最大元素，甚至在 S 是有限时.

例 14.5 (a) 考虑例 14.3 中的三个偏序集，它们的 Hasse 图是图 14－1.

(i) A 有两个极大元素 18 和 24，没有最大元素；A 只有一个极小元素 1，它也是最小元素.

(ii) B 有两个极小元素 d 和 e，没有一个最小元素；B 只有一个极大元素 a，它也是最大元素.

(iii) 链有一个极小元素 x，它是最小元素；还有一个极大元素 v，它也是最大元素.

(b) 设 A 是任一非空集合，$P(A)$ 是带有集合包含关系的 A 的幂集. 那么空集 $\varnothing$ 是 $P(A)$ 的最小元素，因为对于任何集合 X，有 $\varnothing \subseteq X$. 而且，A 是 $P(A)$ 的最大元素，因为 $P(A)$ 中的每一个元素明显地是 A 的一个子集，即 $Y \subseteq A$.

14.4 相容编号

设 S 是一个有限偏序集. 我们希望对 S 中的每一个元素指派一个正整数使得序关系能保持. 即求一个函数 $f: S \to \mathbf{N}$ 使得，如果 $a \prec b$ 那么 $f(a) < f(b)$. 这样的函数被称为 S 的*相容编号*. 下面的定理表明这样的函数是存在的.

定理 14.1 任何有限偏序集 A 存在相容编号.

我们将在问题 14.15 中证明此定理. 其实，只要证明，如果 S 有 n 个元素，那么存在一个相容编号 $f: S \to \{1, 2, \cdots, n\}$.

我们强调这样的编号不是惟一的. 例如，下面是图 14－1(b) 中偏序集的两个编号：

(i) $f(d)=1, f(e)=2, f(b)=3, f(c)=4, f(a)=5$.

(ii) $g(e)=1, g(d)=2, g(c)=3, g(b)=4, g(a)=5$.

然而图 14－1(c) 的链只有一个相容编号，我们把集合 $\{1,2,3,4,5\}$. 并规定：

$$h(x)=1, h(y)=2, h(z)=3, h(u)=4, h(v)=5.$$

14.5 上确界和下确界

设 A 是偏序集 S 的一个子集. S 中元素 M 叫做 A 的一个*上界*，如果 M 后于 A 中的每一

个元素,即如果对 A 中每一个 x 有

$$x \lesssim M.$$

如果 A 的一个上界先于 A 的其他每一个上界,那么它叫做 A 的上确界,表示为

$$\sup(A).$$

如果 A 含有元素 $a_1,\cdots,a_n$,我们也将 $\sup(A)$ 记为 $\sup(a_1,\cdots,a_n)$,我们强调至多只有一个上确界 $\sup(A)$;当然,$\sup(A)$ 也可能不存在.

类似地,偏序集 S 的一个元素 m 叫做 S 的子集 A 的一个下界,如果 m 先于 A 中的每一个元素,即如果对 A 中的每一个 y 有

$$m \lesssim y.$$

如果 A 的一个下界后于 A 的其他每一个下界,那么它叫做 A 的下确界,表示为

$$\inf(A),\text{或} \inf(a_1,a_2,\cdots,a_n)$$

如果 A 含有元素 $a_1,\cdots,a_n$. 我们强调至多只有一个 $\inf(A)$;然而 $\inf(A)$ 也可能不存在.

有些书用最小上界代替上确界,而写作 $\mathrm{lub}(A)$ 不写 $\sup(A)$;用最大下界代替下确界,写作 $\mathrm{glb}(A)$ 不写 $\inf(A)$.

如果 A 有一个上界,我们称 A 是上有界的;如果 A 有一个下界,我们称 A 是下有界的. 特别地,A 是有界的,如果 A 有上界和下界.

例 14.6 (a) $S=\{a,b,c,d,e,f\}$,其序关系由图 14-3(a)表示,设 $A=\{b,c,d\}$. A 的上界是 e,f,因为只有 e 和 f 后于 A 的每一个元素. A 的下界是 a 和 b,因为只有 a 和 b 先于 A 的每一个元素. 注意,e 和 f 是不可比较的,因此 $\sup(A)$ 不存在. 然而 b 也后于 a,因此 $\inf(A)=b$.

(b) $S=\{1,2,3,\cdots,8\}$ 可以用图 14-3(b)表示,设 $A=\{4,5,7\}$. A 的上界是 1,2 和 3,惟一的下界是 8. 注意,7 不是下界,因为 7 不先于 4. 这里 $\sup(A)=3$,因为 3 先于其他上界 1 和 2. 注意,$\inf(A)=8$,因为 8 是惟一的下界.

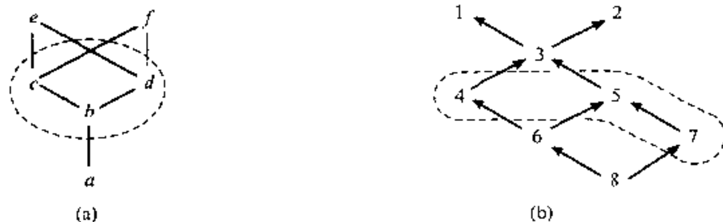


图 14-3

一般地,对偏序集 S 中的任一对元素 a 和 b,$\sup(a,b)$ 和 $\inf(a,b)$ 不一定存在. 下面给出两个偏序集,对任意 a,b,$\sup(a,b)$ 和 $\inf(a,b)$ 都存在.

例 14.7 (a) 设 $\mathbf{N}$ 是在整除关系下的全体正整数集合. $\mathbf{N}$ 中 a 和 b 最大公因数是整除 a 和 b 的最大整数,表示为

$$\gcd(a,b).$$

a 和 b 的最小公倍数是能被 a 和 b 除尽的最小整数,表示为

$$\mathrm{lcm}(a,b).$$

数论中有一个重要定理:a 和 b 的每一个公因数都可以整除 $\gcd(a,b)$. 可以证明 $\mathrm{lcm}(a,b)$ 能整除 a 和 b 的每一个倍数,因此,

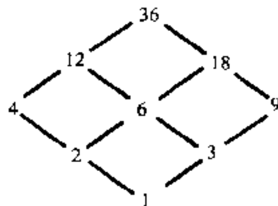


图 14-4

$$\gcd(a,b)=\inf(a,b),\mathrm{lcm}(a,b)=\sup(a,b).$$

换句话说,$\inf(a,b)$ 和 $\sup(a,b)$ 对整除关系的 $\mathbf{N}$ 的每一对元素 a,b 都存在.

(b) 对任何正整数 m,我们用 $\mathbf{D}_m$ 表示 m 的所有因数组成的集合,序关系为整除.

$$\mathbf{D}_{36}=\{1,2,3,4,6,9,12,18,36\}$$

的 Hasse 图在图 14 - 4 中给出. 再者, $\inf(a,b)=\gcd(a,b)$ 和 $\sup(a,b)=\text{lcm}(a,b)$ 对 D_m 中任一对 a,b 都存在.

14.6 同构序集

假设 X 和 Y 是偏序集. A 的单射函数 $f:X\to Y$ 被叫做从 X 到 Y 的相似映射, 如果 f 保持序关系, 即对于 X 中任意元素 a 和 a', 下面两个条件成立:

(1) 若 $a\lesssim a'$, 那么 $f(a)\lesssim f(a')$.

(2) 若 $a\parallel a'$(不可比较的), 那么 $f(a)\parallel f(b)$.

若 A 和 B 是线性序集, 那么只需要条件(1).

两个序集 X 和 Y 是同构的, 如果存在一个保持序关系的双射 $f:X\to Y$, 即一个同构映射 f. 记作

$$X\simeq Y.$$

例 14.8 若 $X=\{1,2,6,8,12\}$ 是在整除关系下的偏序集, $Y=\{a,b,c,d,e\}$ 和 X 同构. 下面的函数 f 是从 X 到 Y 的同构映射

$$f=\{(1,e),(2,d),(6,b),(8,c),(12,a)\}$$

画出 Y 的 Hasse 图.

同构映射保持了初始集 X 的序且是 1 - 1 的和映上的. 因此该映射可认为是初始集 X 的 Hasse 图中顶点的标记. X 和 Y 的 Hasse 图如图 14 - 5.

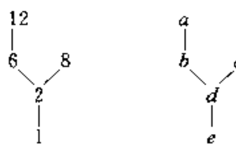


图 14 - 5

14.7 良序集

我们从定义开始.

定义 序集 S 称为良序的, 如果 S 的每一个子集都有最小元素.

良序集的传统例子是带有常序$\leqslant$的正整数集 $\mathbf{N}$. 由定义有下面的事实:

(1) 一个良序集是线性序集. 因为如果 $a,b\in S$, 那么 $\{a,b\}$ 有一个最小元素, 因此 a 和 b 是可比较的.

(2) 良序集的每一个子集都是良序的.

(3) 若 X 是良序的, Y 与 X 同构, 则 Y 也是良序的.

(4) 所有含有 n 个元素的有限线性、序集都是良序的, 且相互同构. 事实上, 它们都与常序$\leqslant$的 $\{1,2,\cdots,n\}$ 是同构.

(5) 对于不是最大元素的任何元素 $a\in S$, 有直接继元. 用 $M(a)$ 表示严格后于 a 的元素集, 那么 $M(a)$ 的最小元素是 a 的直接继元.

例 14.9 (a) 整数集合 $\mathbf{Z}$ 的序$\leqslant$是线性的, 其中的每个元素都有一个直接继元和一个直接前元, 但 $\mathbf{Z}$ 也并不是良序的. 例如, $\mathbf{Z}$ 本身没有最小元素. 然而, 任何有下界的 $\mathbf{Z}$ 的子集都是良序的.

(b) 有理数集合 $\mathbf{Q}$ 的序$\leqslant$是线性的, 但 $\mathbf{Q}$ 中没有元素有直接继元和直接前元. 因为如果 $a,b\in Q$, 比如 $a<b$, 那么有 $(a+b)/2\in Q$ 和

$$a<\frac{a+b}{2}<b.$$

(c) 考虑不交的良序集合:

$$A=\{1,3,5,\cdots\}, B=\{2,4,6,\cdots\}.$$

那么下面的有序集

$$S=\{A;B\}=\{1,3,5,\cdots;2,4,6,\cdots\}$$

是良序集. 注意最小元素是 1 而且元素 2 没有直接前元.

注 从此以后, 如果 $A,B,\cdots$ 是不交有序集, 那么 $\{A;B;\cdots\}$ 意味着集合 $A\cup B\cup\cdots$ 在位置

排序是从左到右的；即相同集合中的元素保持它们自己的顺序，左边集合中的任何元素先于右边集合中的任何元素. 因此，A 中的每个元素都先于 B 中的每个元素，等等.

超限归纳法

首先，我们重述数学归纳法的原理.（见 1.10 和 11.3 节）

数学归纳法原理 设 A 是正整数集合 $\mathbf{N}$ 的一个子集且具有下面两个性质：

(i) $1\in A$.

(ii) 如果 $n\in A$，那么 $n+1\in A$.

则 $A=\mathbf{N}$.

上述原理是 Peano 关于自然数 $\mathbf{N}$ 的公理之一. 它还有一种有时用起来很方便的形式，即

数学归纳法原理（第二种形式） 设 A 是 $\mathbf{N}$ 的子集并具有以下两个性质：

(i) $1\in A$.

(ii) 如果对于 $1\leqslant k<n$，$k\in A$，那么 $n\in A$.

则 $A=\mathbf{N}$.

归纳法的第二种形式和 $\mathbf{N}$ 是良序集（公理 11.6）是等价的. 事实上，有对每一个良序集合都适用的相似的叙述.

超限归纳法原理 设 A 是一个良序集 S 的子集并具有以下两个性质

(i) $a_0\in A$.

(ii) 如果 $s(a)\subseteq A$，那么 $a\in A$.

则 $A=S$.

此处的 a_0 是 S 中的最小元素，$s(a)$ 称为 a 的前缀，即 S 中严格先于 a 的所有元素的集合.

选择公理，良序定理

设 $\{A_i:i\in I\}$ 是一个非空的不交的集簇. 我们假设 $A_i\subseteq X$，函数 $f:\{A_i\}\to X$ 叫做一个选择函数，如果 $f(A_i)=a_i\in A_i$. 换句话说，f 为每个集合 A_i"选择"一点 $a_i\in A_i$.

选择公理是数学尤其是集合论的基础. 这个"表面简单"的公理是数学中的一个有效的重要公理.

选择公理 任何一个非空集合的非空集簇都存在一个选择函数.

选择公理的一个重要推论就是下面的 Zermelo 定理.

良序定理 每一个集合 S 都能成为良序集.

这个定理的证明超出了本书的范围. 此外，因为我们所论结构都是有限的或可数的，我们不必运用这个定理，有普通的数学归纳法就足够了.

14.8 格

设 L 是对二元运算交 $\wedge$ 和并 $\vee$ 封闭的集合. 称 L 为格，如果对 L 中的任意元素 a,b,c，有：

[$\mathbf{L}_1$] 交换律：

(1a) $a\wedge b=b\wedge a$, (1b) $a\vee b=b\vee a$.

[$\mathbf{L}_2$] 结合律：

(2a) $(a\wedge b)\wedge c=a\wedge(b\wedge c)$, (2b) $(a\vee b)\vee c=a\vee(b\vee c)$.

[$\mathbf{L}_3$] 吸收律：

(3a) $a\wedge(a\vee b)=a$, (3b) $a\vee(a\wedge b)=a$.

记 $(L,\wedge,\vee)$ 表示格 L.

对偶律和幂等律

一个格 $(L,\wedge,\vee)$ 中任何一个命题的对偶命题是通过互换 $\wedge$ 和 $\vee$ 得到的. 例如，

$$a\wedge(b\vee a)=a\vee a \text{ 的对偶是 } a\vee(b\wedge a)=a\wedge a.$$

注意格的每个定律的对偶还是格的定律. 由此可得对偶原理,即

定理 14.2(对偶原理) 格中任何一个定理的对偶还是格的一个定理.

格的一个重要的性质可以直接从吸收律得到.

定理 14.3(幂等律) (i) $a\wedge a=a$, (ii) $a\vee a=a$.

(i)的证明只需两行

$$a\wedge a=a\wedge(a\vee(a\wedge b)) \quad (\text{利用(3b)})$$
$$=a. \quad (\text{利用(3a)})$$

条件(ii)的论证可以通过上面的对偶原理(或与(i)类似的证明)得到.

格与序

给出一个格 L,我们可以定义 L 中的偏序如下

$$a\lesssim b, \text{如果 } a\wedge b=a.$$

类似地,我们可以定义

$$a\lesssim b, \text{如果 } a\vee b=b.$$

我们将上述结果叙述为一个定理.

定理 14.4 设 L 是一个格,那么

(i) $a\wedge b=a$ 当且仅当 $a\vee b=b$.

(ii) 关系 $a\lesssim b$(通过 $a\wedge b=a$ 或 $a\vee b=b$ 来定义)是 L 的一个偏序.

现在,在任一个格 L 上我们都有一个偏序,一般地,我们可使 L 图形化,就像偏序集的 Hasse 图一样.

例 14.10 设 C 是一个对交和并封闭的集簇. 那么$(C,\cap,\cup)$是一个格. 在这个格中,偏序关系就是集的包含关系. 图 14-6 为$\{a,b,c\}$的所有子集构成的格的 Hasse 图.

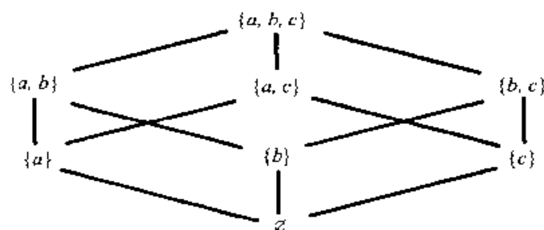


图 14-6

我们已经知道如何在格 L 中定义一个偏序. 下一个定理告诉我们在什么条件下能够在一个偏序集 P 上定义一个格使得这个格能够给出原来的偏序 P.

定理 14.5 设 P 是一个偏序集使得对于任意 $a,b\in P$, $\inf(a,b)$ 和 $\sup(a,b)$ 都存在. 设 $a\wedge b=\inf(a,b)$, $a\vee b=\sup(a,b)$. 我们有$(P,\wedge,\vee)$是一个格. 进一步地,这个格诱导的偏序与原来的偏序 P 相同.

上述定理的逆命题也为真. 即设 L 为一个格,$\lesssim$是在 L 上诱导的偏序. 那么对于任何一对 $a,b\in L$, $\inf(a,b)$ 和 $\sup(a,b)$ 都存在,从偏序集$(L,\lesssim)$获得的格与原来格相同. 于是有

替换定义 一个格是一个偏序集,在这个集合中,对任何一对元素 a 和 b,

$$a\wedge b=\inf(a,b) \text{ 和 } a\vee b=\sup(a,b)$$

都存在.

首先,我们注意到任何线性序集是一个格,因为 $\inf(a,b)=a$ 和 $\sup(a,b)=b$,当 $a\lesssim b$ 时. 根据例 14.7,自然数集 $\mathbf{N}$ 和 m 的因数集 $\mathbf{D}_m$ 在整除关系下是格.

子格，同构格

假设 M 是格 L 的一个非空子集. 我们说 M 是 L 的一个子格，若 M 本身是一个格(关于 L 的运算). 我们注意到 M 是一个子格当且仅当 M 在 L 的 $\wedge$ 和 $\vee$ 的运算下封闭. 例如，m 的因数集 $\mathbf{D}_m$ 在整除关系下是自然数集 $\mathbf{N}$ 的一个子格.

两个格 L 和 L' 被认为是同构的，如果存在一个双射 $f: L \to L'$，使得对 L 中的任何元素 a，b 满足

$$f(a \wedge b) = f(a) \wedge f(b) \text{和} f(a \vee b) = f(a) \vee f(b).$$

14.9　有界格

一个格 L 称为有下界 0，如果对 L 中任何元素 x 都有 $0 \leqslant x$. 类似地，L 称为是有上界 I，如果对 L 中任何元素 x 都有 $x \leqslant I$. 我们说 L 是有界的，如果 L 有下界 0 和上界 I. 在这样的格中，我们有下面的恒等式

$$a \vee I = I, a \wedge I = a, a \vee 0 = a, a \wedge 0 = 0.$$

对 L 中的任意元素 a.

对于非负整数的常序

$$0 < 1 < 2 < 3 < 4 < \cdots$$

有下界为 0，但是没有上界. 另一方面，全集 U 上所有子集构成的格 $P(U)$ 是一个以 U 为上界以 $\varnothing$ 为下界的有界格.

假设 $L = \{a_1, a_2, \cdots, a_n\}$ 是一个有限格，那么

$$a_1 \vee a_2 \vee \cdots \vee a_n \text{和} a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

分别是 L 的上界和下界. 这样我们就有

定理 14.6　每一个有限格 L 都是有界的.

14.10　分配格

格 L 称为分配格，如果对于 L 中任何元素 a, b, c，成立如下定律

[$\mathbf{L}_4$]　分配律：

(4a)　$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$，(4b)　$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

否则，L 是非分配的. 由对偶原理可知(4a)成立当且仅当(4b)成立.

图 14－7(a)是一个非分配格，因为

$a \vee (b \wedge c) = a \vee 0 = a$，但$(a \vee b) \wedge (a \vee c) = I \wedge c = c$.

图 14－7(b)也是一个非分配格. 事实上，对于这样的格有如下特征.

定理 14.7　格 L 是非分配格当且仅当它包含一个形如 14－7(a)或(b)的同构的子格.

这个定理的证明超出本书的范围.

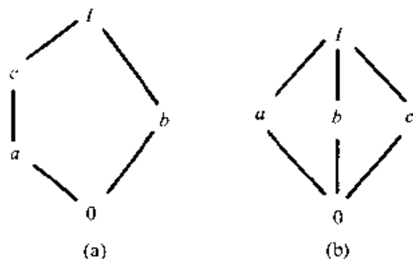


图 14－7

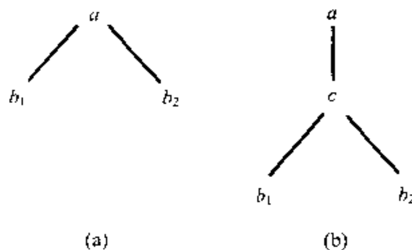


图 14－8

并不可约元素，原子

设 L 是一个以 0 为下界的格. L 中的一个元素 a 称为并不可约的，如果 $a = x \vee y$ 蕴含着

$a=x$或$a=y$.(素数的乘法有这个性质,即如果 $p=ab$,那么 $p=a$ 或 $p=b$,其中 p 是素数.)显然,0 是并不可约的.如果a 至少有 2 个直接前元,如图 14-8(a)中的b_1 和b_2,那么 $a=b_1\vee b_2$,所以 a 不是并不可约的.另一方面,如果 a 有惟一的直接前元 c,那么对任何其他的 b_1,b_2,有 $a\neq\sup(b_1,b_2)=b_1\vee b_2$.因为正如图 14-8(b)所示,$c$ 在 b_1,b_2 与 a 之间.换句话说,a 是并不可约的当且仅当a 有惟一的直接前元.0 的直接继元叫原子,是并不可约的.然而,格可能有其他的并不可约元素.如图 14-7(a)中的 c 不是一个原子,但它是并不可约的,因为 a 是它的惟一的直接前元.

如果一个有限格 L 中的元素a 不是并不可约的,则可以写 $a=b_1\vee b_2$.于是,我们能够把 b_1 和 b_2 写成其他元素的并,如果 b_1,b_2 不是并不可约,等等.因为 L 是有限的,最后有

$$a=d_1\vee d_2\vee\cdots\vee d_n.$$

其中 d_i 都是并不可约的.如果 d_i 先于d_j 那么 $d_i\vee d_j=d_j$.所以可以把 d_i 去掉.也就是说,我们能够假设 d_i 是两两不可比,即没有一个 d_i 先于另一个 d_j.我们强调如此表达并不是惟一的,即在图 14-7 的两个格中均有 $I=a\vee b$ 和 $I=b\vee c$.现在给出本部分的一个主要定理(在问题 14.38 中证明).

定理 14.8 设 L 是一个有限分配格.则 L 中的每一个元素a 都可以惟一(不计顺序)地写成两两不可比的并不可约的元素的并.

事实上,这个定理可以推广到具有有限长度的格,即所有线性序子集都是有限的(在题 14.33 中给出一个长度有限的无限格).

14.11 补元,有补格

设 L 是一个下界为 0 上界为 I 的有界格.a 是L 中的一个元素,L 中的另一元素 x 叫做a 的一个补元,如果

$$a\vee x=I,a\wedge x=0.$$

补元不一定存在也不一定惟一.例如,在图 14-7(a)中元素 a 和c 都是b 的补元.而图 14-1 中的元素 y,z 和 u 都没有补元.我们有下面的结论.

定理 14.9 设 L 是一个有界的分配格.如果补元存在,那么它也是惟一的.

证明 假设 x 和 y 是L 中任意元素 a 的补元,那么

$$a\vee x=I,a\vee y=I,a\wedge x=0,a\wedge y=0.$$

运用分配律

$$x=x\vee 0=x\vee(a\wedge y)=(x\vee a)\wedge(x\vee y)=I\wedge(x\vee y)=x\vee y.$$

类似地,

$$y=y\vee 0=y\vee(a\wedge x)=(y\vee a)\wedge(y\vee x)=I\wedge(y\vee x)=y\vee x.$$

那么

$$x=x\vee y=y\vee x=y.$$

所以定理得证.

有补格

格 L 是有补格,如果L 是有界的且L 中的每一个元素都有补元.如图 14-7(b)中的格是有补格且补元不是惟一的.另一方面,全集 U 中的所有子集构成的格 $P(U)$是有补的,U 中的每个子集A 都有惟一的补元 $A^c=U\setminus A$.

定理 14.10 设 L 是一个有惟一补元的有补格,那么 L 中的并不可约元素除 0 以外是它的原子.

结合本定理与定理 14.8 和 14.9,我们得如下重要结论.

定理 14.11 设 L 是一个有限的有补分配格,那么 L 中的每一个元素 a 都可写成惟一的原子集合的并.

注　有些书定义当 L 中每一个元素 a 都有惟一的补元时 L 为有补格. 因此定理 14.10 的叙述有所不同.

问题与解答

有序集和有序子集

14.1　假设自然数集合 $\mathbf{N}=\{1,2,3,\cdots\}$ 是整除关系下的偏序集. 在下面两个数中间填上正确的符号, $\prec$, $\succ$ 或 $\|$ (不可比较的).

(a) 2 ____ 8; (b) 18 ____ 24; (c) 9 ____ 3; (d) 5 ____ 15.

解　(a) 因为 2 整除 8, 2 先于 8, 即 $2\prec 8$.

(b) 18 不能整除 24, 24 不能整除 18; 所以 $18 \| 24$.

(c) 因为 9 被 3 整除, $9\succ 3$.

(d) 因为 5 整除 15, $5\prec 15$.

14.2　设 $\mathbf{N}=\{1,2,3,\cdots\}$ 是整除关系下的偏序集, 说明下列 $\mathbf{N}$ 的子集是否是线性序集.

(a) $\{24,2,6\}$;　(b) $\{3,15,5\}$;　(c) $N=\{1,2,3,\cdots\}$;

(d) $\{2,8,32,4\}$;　(e) $\{7\}$;　(f) $\{15,5,30\}$.

解　(a) 因为 2 整除 6, 6 又整除 24, 是线性序集.

(b) 因为 3 和 5 不可比较, 不是线性序集.

(c) 因为 2 和 3 不可比较, 不是线性序集.

(d) 是线性序集, 因为 $2\prec 4\prec 8\prec 32$.

(e) 任何只有一个元素的集合都是线性序集.

(f) 因为 5 整除 15, 15 又整除 30, 是线性序集.

14.3　设 $A=\{1,2,3,4,5\}$ 的序关系如 Hasse 图 14-9 所示. 在下列每对元素之间填上正确的符号 $\prec$, $\succ$ 或 $\|$ (不可比较的).

(a) 1 ____ 5; (b) 2 ____ 3; (c) 4 ____ 1; (d) 3 ____ 4

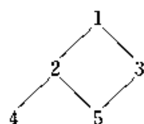


图 14-9

解　(a) 因为有一路线从 5 到 3 到 1, 5 先于 1, 所以 $1\succ 5$.

(b) 因为没有从 2 到 3 的路, 所以 $2 \| 3$.

(c) 因为有一路从 4 到 2 到 1, 所以 $4\prec 1$.

(d) 既没有 $3\prec 4$ 也没有 $4\succ 3$, 所以 $3 \| 4$.

14.4　考虑图 14-9 中的序集 A.

(a) 求 A 中的极大元素和极小元素.

(b) A 有最小元素和最大元素吗?

解　(a) 没有元素严格先于 4 或 5, 所以 4 和 5 是 A 的极小元素, 没有元素严格地在 1 的后面, 所以 1 是 A 中的一个极大元素.

(b) A 中没有最小元素. 虽然 4 和 5 是 A 中的极小元素, 但两个中没有一个先于另一个. 然而, 1 是 A 中的一个最大元素, 因为 1 在 A 中所有元素的后面.

14.5　考虑图 14-9 中的序集 A. $L(A)$ 指的是 A 中所有具有 2 个或 2 个以上的元素的线性序子集的集合. $L(A)$ 是包含关系的偏序集. 画出 $L(A)$ 的 Hasse 图.

解　$L(A)$ 的元素如下

$\{1,2,4\},\{1,2,5\},\{1,3,5\},\{1,2\},\{1,4\},\{1,3\},\{1,5\},\{2,4\},\{2,5\},\{3,5\}$.

(注意, $\{2,3\}$ 和 $\{3,4\}$ 不是线性序集.) $L(A)$ 的 Hasse 图如图 14-10.

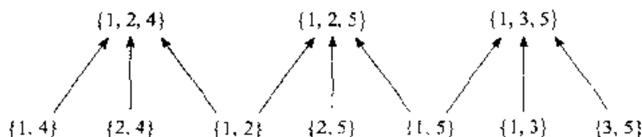


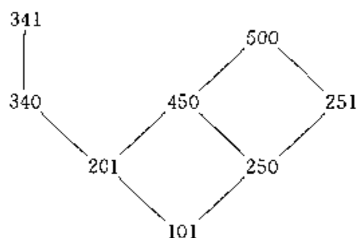
图 14-10

14.6 大学中预备课程关系是熟知的可选课程上的偏序关系. 我们说 $A \ll B$,如果课程 A 对于课程 B 来说是必要的. 考虑图 14－11(a)中数学课程和它们的预备课,画出这些课程的偏序关系的 Hasse 图.

解 ☞ 数学 101 是在图的底部,因为它是惟一不要预备课程的. 因为数学 201 和数学 250 仅仅要求数学 101,我们有数学 101≪数学 201,数学 101≪数学 250;所以画一条向上的线从数学 101 到数学 201,再画另一条从数学 101 到数学 250 的向上的线,继续这样的过程,我们可以得到如图 14－11(b)的 Hasse 图.

课程	所需预备课程
数学 101	无
数学 201	数学 101
数学 250	数学 101
数学 251	数学 250
数学 340	数学 201
数学 341	数学 340
数学 450	数学 201,数学 250
数学 500	数学 450,数学 251

(a)



(b)

图 14－11

14.7 考虑关于数学课的偏序集合 C,如图 14－11.

(a) 求 C 中的所有的极小元素和极大元素.

(b) C 有最小元素和最大元素吗?

解 ☞ (a) 没有元素严格先于数学 101,所以数学 101 是 C 的一个极小的元素. 没有元素严格地后于数学 341 或数学 500,所以数学 341 或数学 500 是 C 的极大元素.

(b) 数学 101 是 C 的最小元素,因为它先于 C 中的任何一个其他元素. 然而 C 没有最大的元素,虽然数学 341 和数学 500 是极大元素,但都不是最大元素,因为它们都不先于它们中的另一个元素.

14.8 考虑正整数集合 $\mathbf{N}=\{1,2,3,\cdots\}$,$\mathbf{N}$ 中的每个数都可以惟一地写成 2 的非负整数幂与一个奇数的乘积. 假设 a 和 a' 都是正整数,如

$$a=z^{r}(2s+1) \text{和} a'=z^{r'}(2s'+1).$$

其中 r 和 s 是非负整数. 我们定义

$$a \prec a', \text{如果 } r<r', \text{或者 } r=r', \text{但 } s<s'.$$

在下面各对数之间填入符号"$\succ$"或"$\prec$"

(a) 5 ____ 14;(b) 6 ____ 9;(c) 3 ____ 20;(d) 14 ____ 21.

解 ☞ $\mathbf{N}$ 中元素如图 14－12 排列;第一行是奇数,第二行是上述奇数的 2 倍,第三行是 $2^2=4$ 倍的奇数,依次类推. 因此,若 a 在比 a' 高的行里,则 $a \prec a'$;若 a 和 a' 在同一行中,但 a 在 a' 的前面,则 $a \prec a'$. 例如

r \ s	0	1	2	3	4	5	6	7	
0	1	3	5	7	9	11	13	15	…
1	2	6	10	14	18	22	26	30	…
2	4	12	20	28	36	44	52	60	…
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

图 14－12

(a) $5 \prec 14$;(b) $6 \succ 9$;(c) $3 \succ 20$;(d) $14 \succ 21$.

集合的积和序

14.9　设积序集 $N^2=N\times N$，这里 N 是常序集. 在下列每对 $N\times N$ 元素之间填入符号"$\prec$"、"$\succ$"或"$\|$"(不可比较).

(a) (5,7)______(7,1)；

(b) (4,6)______(4,2)；

(c) (5,5)______(4,8)；

(d) (1,3)______(1,7)；

(e) (7,9)______(4,1)；

(f) (7,9)______(8,2).

解 这里 $(a,b)\precsim(a',b')$ 当且仅当 $a\leqslant a',b\leqslant b'$. 从而当 $a<a',b\leqslant b'$ 或 $a\leqslant a',b<b'$ 时有 $(a,b)\prec(a',b')$ 因此，

(a) $\|$：因为 $5<7$ 但 $7>1$；

(b) $\succ$：因为 $4\geqslant4$ 且 $6>2$；

(c) $\|$：因为 $5>4$ 但 $5<8$；

(d) $\prec$：因为 $1\leqslant1$ 且 $3<7$；

(e) $\succ$：因为 $7>4$ 且 $9>1$；

(f) $\|$：因为 $7<8$ 但 $9>2$.

14.10　设 $N^2=N\times N$ 是字典排序集，重做 14.9 中的问题.

解 这里 $(a,b)\prec(a',b')$ 当且仅当 $a<a'$ 或 $a=a'$ 但 $b<b'$.

(a) $\prec$：因为 $5<7$；(b) $\succ$：因为 $4=4$ 且 $6>2$；

(c) $\succ$：因为 $5>4$；(d) $\prec$：因为 $1=1$ 且 $3<7$；

(e) $\succ$：因为 $7>4$；(f) $\prec$：因为 $7<8$.

14.11　设英文字母排序集 $A=\{a,b,c,\cdots,y,z\}$，$A^2=A\times A$ 是积序集. 下面是两个字母的字符串(看作 $A\times A$ 的元素)，在每对中间填入"$\succ$"，"$\prec$"或"$\|$".

(a) cx ______ at；(b) cx ______ by；(c) cx ______ cz；

(d) cx ______ rs；(e) cx ______ dx；(f) cx ______ cs.

解 (a) $\succ$：因为 $c>a$ 且 $x>t$.

(b) $\|$：因为 $c>b$ 但 $x<y$.

(c) $\prec$：因为 $c\leqslant c$ 且 $x<z$.

(d) $\|$：因为 $c<r$ 但 $x>s$.

(e) $\prec$：因为 $c<d$ 且 $x\leqslant x$.

(f) $\succ$：因为 $c\leqslant c$ 且 $x>s$.

14.12　设 $A^2=A\times A$ 是字典排序集，重做问题 14.11.

解 (a) $\succ$：因为 $c>a$.

(b) $\succ$：因为 $c>b$.

(c) $\prec$：因为 $c=c$ 且 $x<z$.

(d) $\prec$：因为 $c<r$.

(e) $\prec$：因为 $c<d$.

(f) $\succ$：因为 $c=c$ 且 $x>s$.

14.13　设英文字母排序集 $A=\{a,b,c,\cdots,y,z\}$，A^* 由 A 中所有字符串组成并赋予字典(自由半群)长度序. 把下列单词(字符串)排序：

went, forget, to, medicine, me, toast, melt, for, me, arm

解 首先按字母长度排序，然后再按字母表顺序排序：

me, to, we, arm, for, melt, went, toast, forget, medicine

14.14　按正常的字母表顺序将问题 14.13 中的字符串排序.

解 ☞ 正常顺序为：arm, for, forget, me, medicine, melt, to, toast, we, went

相容编号

14.15 设序集 $S=\{a,b,c,d,e\}$，序关系如图 14-13 所示. 求所有 $f:S\to\{1,2,3,4,5\}$ 的相容编号.

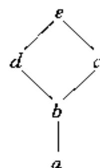


图 14-13

解 ☞ 因为 a 是惟一极小元素，从而 $f(a)=1$，又因为 e 是惟一极大元素，从而 $f(e)=5$. 又 $f(b)=2$，因为 b 是 a 的直接继元. 从而 $f(c)=3, f(d)=4$ 或者 $f(c)=4, f(d)=3$，因此有两种可能的编号. 如下：

(i) $f(a)=1, f(b)=2, f(c)=3, f(d)=4, f(e)=5$.

(ii) $f(a)=1, f(b)=2, f(c)=4, f(d)=3, f(e)=5$.

我们强调通常不能从一个给定的相容编号中再产生原先的编序.

14.16 证明定理 14.1：假设 S 是有 n 个元素的有限偏序集，那么存在一个相容编号 $f:S\to\{1,2,\cdots,n\}$.

证 ☞ 对 S 中 n 个元素进行归纳证明. 假设 $n=1, S=\{s\}$，那么 $f(s)=1$ 是 S 的一个相容编号. 现在假设 $n>1$，定理对于少于 n 个元素的偏序集成立. 设 S 中的 a 为极小元素.（如此的元素 a 是存在的，因为 S 是有限的.）设 $T=S\setminus\{a\}$，那么 T 是有 $n-1$ 个元素的有限偏序集，因此根据归纳假设，T 有一个相容编号，比如 $g:T\to\{1,2,\cdots,n-1\}$. 由

$$f(x)=\begin{cases}1, 若\ x=a,\\ g(x)+1, 若\ x\neq a\end{cases}$$

定义 $f:S\to\{1,2,\cdots,n\}$，

则 f 是所求的相容编号.

14.17 假设一个学生想在问题 14.6 中选所有的 8 门数学课程，但每学期一门.

(a) 哪些课程是她第一或最后一学期（第八学期）选择的？

(b) 假如她想在第一年（第一或第二学期）中选数学 250，在第四年（第七或第八学期）选数学 340，找出所有她选 8 门数学课程的方法.

解 ☞ (a) 按图 14-11，数学 101 是惟一极小的课程，因此必须在第一学期选，数学 341 和 500 是极大的课程，因此其中之一必须在最后一学期选.

(b) 数学 250 不是极小的课程，因此在第二学期选；数学 340 不是极大的课程，因此在第七学期选；数学 341 在第八学期选. 数学 500 必须在第六学期选. 下面给出选 8 门课可能的方法：

[101, 250, 251, 201, 450, 500, 340, 341].

[101, 250, 201, 251, 450, 500, 340, 341].

[101, 250, 201, 450, 251, 500, 340, 341].

上界和下界，上确界和下确界

14.18 设序集 $S=\{a,b,c,d,e,f,g\}$，序关系如图 14-14(a) 所示，设 $X=\{c,d,e\}$.

(a) 找出 X 的上界和下界.

(b) 确定 X 的上确界 $\sup(x)$ 和 X 的下确界 $\inf(X)$，如果存在的话.

解 ☞ 元素 e, f, g 后于 X 中的每个元素；因此 e, f, g 是 X 的上界. 元素 a 先于 X 中的每个元素. 因此它是 X 的下界. 注意 b 不是 X 的下界，因为 b 不先于 c；事实上，b, c 是不可比较的.

因为 e 先于 f 和 g，所以 $e=\sup(X)$，同样，因为 a 后于 X 的每个下界，所以 $a=\inf(X)$，注意 $\sup(X)$ 属于 X，但 $\inf(X)$ 不属于 X.

14.19 设序集 $S=\{1,2,3,\cdots,8\}$，序关系如图 14-14(b) 所示，设 $A=\{2,3,6\}$.

(a) 求 A 的上界和下界.

(b) 确定 A 的上确界和下确界，如果都存在的话.

解 ☞ (a) 上界是 2，下界是 6 和 8.

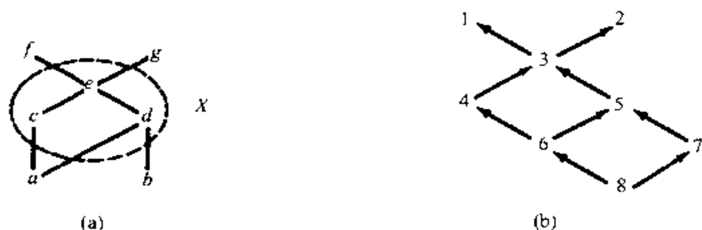


图 14－14

(b) A 的上确界为 2，下确界为 6.

14.20 对子集 $B=\{1,2,5\}$，重做问题 14.19.

解 (a) B 没有上界，因为没有元素后于 1 和 2，下界为 5，6，7，8.

(b) 显然，A 的上确界不存在，因为没有上界. 下确界为 5.

14.21 设序集 $\mathbf{Q}$ 是有理数集，序关系为常序. 设 $D=\{x:x\in\mathbf{Q},8<x^3<15\}$ 是 $\mathbf{Q}$ 的子序集.

(a) D 有上界或者下界吗?

(b) 上确界、下确界存在吗?

解 (a) D 存在上界和下界，例如：1 是下界，100 是上界.

(b) D 的上确界不存在，假设 D 有上确界 x，因为 $\sqrt[3]{15}$ 是无理数，$x>\sqrt[3]{15}$. 但是，存在有理数 y 使得 $\sqrt[3]{15}<y<x$，因此 y 是 D 的一个上界，这与假设 D 的上确界为 x 矛盾. 另一方面，D 的下确界存在，即 $\inf(D)=2$.

同构序集，同构映射

14.22 假设偏序集 A 与 B 同构：$f:A\to B$ 是同构映射，下面的说法对吗?

(a) 元素 $a\in A$ 是 A 的最小(最大，极小或极大)的元素，当且仅当 $f(a)$ 是 B 中最小(最大，极小或极大)的元素.

(b) 元素 $a\in A$ 直接先于元素 $a'\in A$，即 $a\ll a'$ 当且仅当 $f(a)\ll f(a')$.

(c) 元素 $a\in A$，有 A 中的直接继元 r，当且仅当 $f(a)$ 在 B 中存在直接继元 $f(r)$.

解 上述说法均正确，A，B 的结构顺序相同.

14.23 设有序集 S 如图 14－13 所示. 假设 $A=\{1,2,3,4,5\}$ 与 S 是同构的且 $f=\{(a,1)(b,3)(c,5)(d,2)(e,4)\}$ 是从 S 到 A 的同构映射，画出 A 的 Hasse 图.

解 同构映射 f 保持 S 的序结构，因此 f 可以简单地看作是 S 的 Hasse 图中结点的重新标记. 图 14－15 表示 A 的 Hasse 图.

14.24 设有序集 $A=\{1,2,3,4,5\}$ 如图 14－15 所示. 求同构映射 $f:A\to A$ 的个数 n.

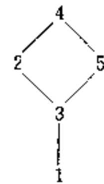


图 14－15

解 因为 1 是 A 中惟一极小的元素，4 是惟一极大的元素，所以必须有 $f(1)=1$，$f(4)=4$. 同样，$f(3)=3$，因为 3 是 1 的惟一的后继元. 另一方面，$f(2)$，$f(5)$ 有两种可能，即 $f(2)=2$，$f(5)=5$. 或 $f(2)=5$，$f(5)=2$，因此 $n=2$.

14.25 求一个与 $Y=(A,R^{-1})$ 同构的有限非线性序集 $X=(A,R)$.

解 如图 14－16(a)，设 R 是 $A=\{a,b,c,d,e\}$ 的偏序. 图 14－16(b) 表示 A 的逆序 R^{-1} (R 的图简单地翻转变成 R^{-1}) 注意两个图除标记外完全相同.

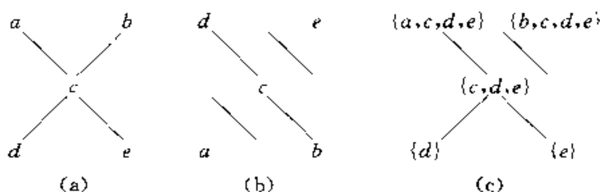


图 14 - 16

14.26 设 A 为有序集. 对于 $a\in A$,$p(a)$表示 a 的前元的集合:$p(a)=\{x:x\lesssim a\}$(称为 a 的前元集),设有序集 $p(A)=\{p(a):a\in A\}$,序关系为集合的包含关系.

(a) 证明 A 和 $p(A)$是同构的,方法是通过证明映射 $f:A\to p(A)$. 是 A 到 $p(A)$的同构映射,这里 $f(a)=p(a)$.

(b) 求图 14 - 16(a)中的集合 A 对应的 $p(A)$的 Hasse 图.

证 (a) 首先,证明 f 保持 A 的序关系. 假设 $a\lesssim b$. 若 $x\in p(a)$,则 $x\lesssim a$,从而 $x\lesssim b$. 因此 $x\in p(b)$. 于是 $p(a)\subseteq p(b)$. 假设 $a\parallel b$(不可比较),则 $a\in p(a)$,但 $a\notin p(b)$;因此 $p(a)\nsubseteq p(b)$. 类似地,$b\in p(b)$. 但 $b\notin p(a)$,从而 $p(b)\nsubseteq p(a)$. 因此,$p(a)\parallel p(b)$. 于是 f 保持序关系.

以下只需证明 f 是单射和满射. 假设 $y\in p(A)$,那么对某个 $a\in A$ 有 $y=p(a)$,因此,$f(a)=p(a)=y$,所以 f 是到 $p(A)$上的满射. 假设 $a\neq b$,则 $a\prec b$,$b\prec a$ 或 $a\parallel b$. 在前段第三种情况下,$b\in p(b)$但 $b\notin p(a)$,在第二种情况下,$a\in p(a)$但 $a\notin p(b)$,总之,在三种情况下,有 $p(a)\neq p(b)$,因此 f 是单射.

于是,f 是 A 到 $p(A)$的同构映射,即 $A\simeq p(A)$.

(b) $p(A)$的元素如下

$p(a)=\{a,c,d,e\}$,$p(b)=\{b,c,d,e\}$,

$p(c)=\{c,d,e\}$,$p(d)=\{d\}$,$p(e)=\{e\}$.

图 14 - 16(c)按集合包含关系给出了 $p(A)$的 Hasse 图. 注意图 14 - 16(a)和(c)除标记外是相同的.

良序集

14.27 证明超限归纳原理:设 A 是良序集合 S 的一个子集且具有两个性质:

(1) $a_0\in A$;(2) 若 $S(a)\subseteq A$,则 $a\in A$. 那么 $A=S$.

证 (这里 a_0 是 A 中最小元素,$S(a)$是 a 的前缀,即所有严格地先于 a 的元素的集合). 假设 $A\neq S$,设 $B=S\setminus A$,则 $B\neq\varnothing$. 因为 S 是良序的,B 有最小元素 b_0. 每一 $x\in S(b_0)$的元素先于 b_0 且不属于 B. 这样每一 $x\in S(b_0)$属于 A,即 $S(b_0)\subseteq A$. 由(2),$b_0\in A$,这与假设 $b_0\in S\setminus A$ 矛盾. 这样最初的假设 $A\neq S$ 是错误的,因而 $A=S$.

14.28 设 S 是以 a_0 为最小元素的良序集. 定义 S 的极限元素.

解 如果 $b\neq a_0$ 而且 b 没有直接前元,那么称元素 $b\in S$ 是一个极限元素.

14.29 设 $S=(\mathbf{N},\lesssim)$是问题 14.8 中的偏序集见图 14 - 12. S 有极限元素吗?

解 如图 14 - 12 所示,每一个 2 的幂,即 1,2,4,8…没有直接前元,因此是 S 的极限元素.

14.30 设 S 是一良序集. 设 $f:S\to S$ 是 S 到 S 的一个相似映射. 证明:对于每个 $a\in S$,有 $a\lesssim f(a)$.

证 设 $D=\{x:f(x)\prec x\}$,若 D 为空集,则命题成立. 若 $D\neq\varnothing$,因为 D 是良序集,D 有最小元素 d_0. 因为 $d_0\in D$,有 $f(d_0)\prec d_0$. 因为 f 是一个相似映射:$f(d_0)\prec d_0$ 蕴含 $f(f(d_0))\prec f(d_0)$. 因此,$f(d_0)$也属于 D,但 $f(d_0)\prec d_0$ 且 $f(d_0)\in D$ 与 d_0 是 D 的最小元素矛盾. 因此最初的假设 $D\neq\varnothing$ 不成立. 所以 D 是空集,命题成立.

14.31 设 A 是一良序集. 设 $s(A)$表示在集合包含关系下所有 A 中元素 a 的前缀 $s(a)$的集合. 证明 A 与 $s(A)$同构,证明方法是证明映射 $f:A\to s(A)$是 $A\to s(A)$的同构映射,这里 $f(a)=s(a)$. (与 14.26 比较).

证 首先证明 f 是双射,假设 $y\in s(A)$. 那么对于某个 $a\in A$,有 $y=s(a)$,因此 $f(a)=s(a)=$

y. 从而 f 是 $s(A)$ 的满射. 假设 $x\neq y$，那么一个先于另一个，比如说 $x\prec y$. 那么 $x\in s(y)$，但 $x\notin s(x)$，因此，$s(x)\neq s(y)$. 因此 f 也是单射.

现在只要证明 f 保持序关系，即 $x\lesssim y$ 当且仅当 $s(x)\subseteq s(y)$. 假设 $x\lesssim y$，如果 $a\in s(x)$. 那么 $a\prec x$ 并且 $a\prec y$；因此 $a\in s(y)$，$s(x)\subseteq s(y)$. 另一方面，假设 $x\not\lesssim y$，即 $x\succ y$. 那么 $y\in s(x)$. 但 $y\notin s(y)$；因此 $s(x)\nsubseteq s(y)$. 换句话说，$x\lesssim y$ 当且仅当 $s(x)\subseteq s(y)$. 于是 f 是 A 到 $s(A)$ 的同构映射. 因此 $A\simeq s(A)$.

格

14.32 写出下列命题的对偶命题.

(a) $(a\wedge b)\vee c=(b\vee c)\wedge(c\vee a)$；

(b) $(a\wedge b)\vee c=a\wedge(b\vee a)$.

解 ☞ 用 $\wedge$ 代替 $\vee$，用 $\vee$ 代替 $\wedge$，得到对偶命题：

(a) $(a\vee b)\wedge c=(b\wedge c)\vee(c\wedge a)$；

(b) $(a\vee b)\wedge a=a\vee(b\wedge a)$.

14.33 求一个有有限长度的无限格 L 的例子.

解 ☞ 设 $L=\{0,1,a_1,a_2,a_3,\cdots\}$，$L$ 按图14-17排序. 即对于 $n\in\mathbf{N}$，有 $0<a_n<1$，因此 L 有有限长度，因为 L 没有无限线性子序集.

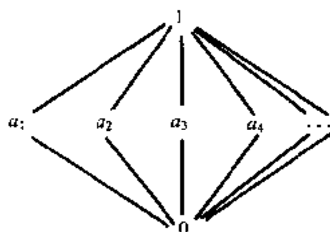


图 14-17

14.34 证明定理 14.4：设 L 是一个格，那么

(i) $a\wedge b=a$ 当且仅当 $a\vee b=b$.

(ii) $a\lesssim b$（由 $a\wedge b=a$ 或 $a\vee b=b$ 定义）是 L 上的偏序关系.

证 ☞ (i) 假设 $a\wedge b=a$，第一步由吸收律得

$$b=b\vee(b\wedge a)=b\vee(a\wedge b)=b\vee a=a\vee b.$$

现假设 $a\vee b=b$，再一次用吸收律得

$$a=a\wedge(a\vee b)=a\wedge b.$$

因此 $a\wedge b=a$ 当且仅当 $a\vee b=b$.

(ii) 对于 L 中任一元素 a，根据幂等律有 $a\wedge a=a$，因此 $a\lesssim a$，从而 $\lesssim$ 是反射性的.

假设 $a\lesssim b$ 和 $b\lesssim a$，那么 $a\wedge b=a$ 和 $b\wedge a=b$，因此 $a=a\wedge b=b\wedge a=b$. 从而 $\lesssim$ 是反对称的.

最后，假设 $a\lesssim b$ 和 $b\lesssim c$，那么 $a\wedge b=a$ 和 $b\wedge c=b$.

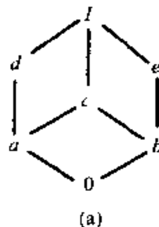
因此，$a\wedge c=(a\wedge b)\wedge c=a\wedge(b\wedge c)=a\wedge b=a$.

因此，$a\lesssim c$ 从而 $\lesssim$ 是传递性的.

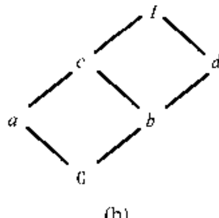
于是，$\lesssim$ 是关于 L 的偏序关系.

14.35 图 14-18 中哪些偏序集合是格？

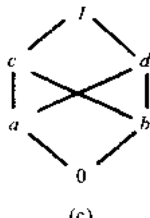
解 ☞ 一偏序集合是格当且仅当 $\sup(x,y)$，$\inf(x,y)$ 对于集合中的每对 x,y 均存在. 只有(c)不是格，因为 $\{a,b\}$ 有 3 个上界 c,d,I，其中无一先于其他两个. 即：$\sup(a,b)$ 不存在.



(a)



(b)



(c)

图 14-18

14.36 考虑图 14-18(a)中的格 L，

(a) 哪些非 0 元素是并不可约的？

(b) 哪些元素是原子？

(c) 下面哪些是 L 的子格.

$L_1=\{0,a,b,I\}$,　　$L_2=\{0,a,e,I\}$,

$L_3=\{a,c,d,I\}$,　　$L_4=\{0,c,d,I\}$.

(d) L 是分配格吗?

(e) 若存在,求元素 a,b,c 的补元.

(f) L 有补格吗?

解 ☞ (a) 有惟一的直接前元的非零元素是并不可约的,因此 a,b,d 和 e 是并不可约的.

(b) 有直接后于 0 的元素是原子,所以 a,b 是原子.

(c) 如果 L' 对 $\wedge$, $\vee$ 封闭时,L' 是 L 的一子格,L_1 不是子格,因为 $a\vee b=c$,c 不属于 L_1. L_4 不是子格,因为 $c\wedge d=a$ 不属于 L_4. 另两个集合 L_2 和 L_3 是子格.

(d) L 不是分配格,因为 L 的子格 $M=\{0,a,d,e,I\}$ 同构于图 14-7(a)所示的非分配格.

(e) 我们有 $a\wedge e=0$,$a\vee e=I$,所以 a 和 e 是互补的元. 同样,b 和 d 是互补元. 而 c 没有补元.

(f) L 不是有补格,因为 c 没有补元.

14.37 考虑图 14-18(b)中的格 M.

(a) 求 M 中非零并不可约元素和原子.

(b) M 是分配格吗?

(c) M 是有补格吗?

解 ☞ (a) 有惟一直接前元的非 0 元素是 a,b,d,其中只有 a 和 b 是原子,因为 a 和 b 的惟一直接前元是 0.

(b) M 是分配格,因为 M 没有与图 14-7 同构的子格.

(c) M 不是有补格,因为 b 没有补元,注意 a 是惟一的适合 $b\wedge x=0$ 的解,但 $b\vee a=c\neq I$.

14.38 证明定理 14.8:设 L 是有限分配格,那么 L 中每一个 a 能惟一地写为两两不可比的并不可约元素的并.

证 ☞ 因为 L 是有限的,可仿照 14.9 节的讨论写成两两不可比的并不可约元素的并. 因此我们只需证明惟一性. 假设

$$a=b_1\vee b_2\vee\cdots\vee b_r=c_1\vee c_2\vee\cdots\vee c_s,$$

这里 $b_1,b_2,\cdots,b_r$ 和 $c_1,c_2,\cdots,c_s$ 都是两两不可比较的并不可约的. 对于一给定的 i 有

$$b_i\precsim(b_1\vee b_2\vee\cdots\vee b_r)=(c_1\vee c_2\vee\cdots\vee c_s).$$

因此

$$b_i=b_i\wedge(c_1\vee c_2\vee\cdots\vee c_s)=(b_i\wedge c_1)\vee(b_i\wedge c_2)\vee\cdots\vee(b_i\wedge c_s).$$

因为 b_i 是并不可约的,存在一个 j 使 $b_i=b_i\wedge c_j$,从而 $b_i\precsim c_j$,类似地,$c_j\precsim b_k$,因此

$$b_i\precsim c_j\precsim b_k.$$

因为 $b_1,b_2,\cdots,b_r$ 是两两不可比的,从而 $b_i=c_j=b_k$. 因此定理得证.

14.39 证明定理 14.10:设 L 是有惟一补元的有补格,那么 L 的并不可约元素(除 0 以外)是它的原子.

证 ☞ 假设 a 是并不可约的但不是原子,那么 a 有惟一直接前元 $b\neq 0$,设 b' 是 b 的补元,因为 $b\neq 0$,我们有 $b'\neq I$. 若 a 先于 b',则 $b\precsim a\precsim b'$,从而 $b\wedge b'=b'$,这是不可能的,因为 $b\wedge b'=0$. 因此 a 不先于 b'. 从而 $a\wedge b'$ 一定严格先于 a. 因为 b 是 a 的惟一直接前元,我们也有 $a\wedge b'$ 先于 b(如图 14-19). 但 $a\wedge b'$ 先于 b'. 因此,

$$a\wedge b'\precsim\inf(b,b')=b\wedge b'=0$$

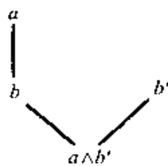


图 14-19

因此 $a\wedge b'=0$.

因为 $a\vee b=a$,又有

$$a\vee b'=(a\vee b)\vee b'=a\vee(b\vee b')=a\vee I=I.$$

因此 b' 是 a 的一个补元. 因为补元是惟一的,$a=b$. 这与假设 b 是 a 直接前元相矛盾. 从而惟一的并不可约元素是它的原子.

补　充　题

有序集和有序子集

14.40　设序集 $A=\{1,2,3,4,5,6\}$，如图 14 - 20(a)所示.

(a) 求 A 中所有极小和极大元素.

(b) A 有最小或最大元素吗？

(c) 求所有 A 的线性序子集，每个子集至少有 3 个元素.

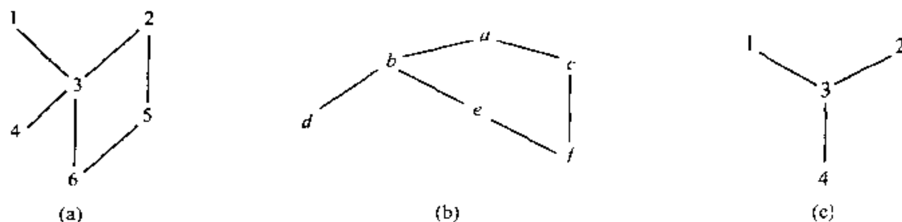


图 14 - 20

14.41　设序集 $B=\{a,b,c,d,e,f\}$，如图 14 - 20(b)所示.

(a) 求 B 中极小，极大的元素.

(b) B 有最小或最大元素吗？

(c) 求 B 到集合$\{1,2,3,4,5,6\}$的相容编号的种数.

14.42　设有序集 $C=\{1,2,3,4\}$，如图 14 - 20(c)所示. 设 $L(C)$表示集合包含关系下的所有 C 的非序的线性序子集的集合，画出 $L(C)$的 Hasse 图.

14.43　画出 m 的划分的 Hasse 图(参照例 14.14).

(a) $m=4$；(b) $m=6$.

14.44　设 $\mathbf{D}_m$ 表示整除关系下 m 的正因数的集合. 画出 Hasse 图

(a) $\mathbf{D}_{12}$；(b) $\mathbf{D}_{15}$；(c) $\mathbf{D}_{16}$；(d) $\mathbf{D}_{17}$.

14.45　设 $S=\{a,b,c,d,e,f\}$是偏序集. 假设恰有六对元素第一个直接先于第二个：

$f \ll a, f \ll d, e \ll b, c \ll f, e \ll c, b \ll f$.

(a) 求 S 中所有极小、极大的元素.

(b) S 有最小或最大的元素吗？

(c) 如果有的话，求不可比较的元素偶.

14.46　判定下列命题是真命题还是假命题，如果是假命题，请给出反例.

(a) 若偏序集 S 只有一个极大元素 a，则是最大元素.

(b) 若有限偏序集 S 只有一个极大元素 a，则 a 是最大元素.

(c) 若一线性序子集 S 只有一极大元素 a，则 a 是最大元素.

14.47　设序集 $S=\{a,b,c,d,e\}$，如图 14 - 21(a)所示.

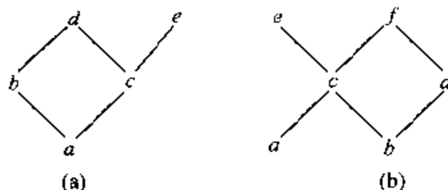


图 14 - 21

(a) 求 S 中所有极小、极大元素.

(b) S 中有最小或最大的元素吗？

(c) 求 S 的所有子集，且 c 是它的极小元素.

(d) 求 S 的所有子集，且 c 是它的最小元素.

(e) 列出所有有 3 个或 3 个以上元素的线性序子集.

14.48　设序集 $S=\{a,b,c,d,e,f\}$，如图 14 - 21(b)所示.

(a) 求 S 中所有极大、极小的元素.

(b) S 中有最小或最大元素吗?

(c) 列举 3 个或 3 个以上元素的线性序子集.

14.49 设序集 $S=\{a,b,c,d,e,f,g\}$,如图 14-14(a)所示,求 S 中的:(a) 4 个元素;(b) 5 个元素的线性序子集的数目 n.

14.50 设序集 $S=\{1,2,\cdots,7,8\}$,如图 14-14(b)所示,求 S 中的:(a) 5 个元素;(b) 6 个元素的线性序子集的数目 n.

相容编号

14.51 设 $S=\{a,b,c,d,e\}$,如图 14-21(a)所示,列举用$\{1,2,3,4,5\}$对 S 的所有相容编号.

14.52 设 $S=\{a,b,c,d,e,f\}$,如图 14-21(b)所示,求用$\{1,2,3,4,5,6\}$对 S 的相容编号的个数 n.

14.53 假设下列为有序集 $A=\{a,b,c,d\}$的 3 个相容编号:$[(a,1),(b,2),(c,3),(d,4)]$, $[(a,1),(b,3),(c,2),(d,4)]$, $[(a,1),(b,4),(c,2),(d,3)]$,假设 A 的 Hasse 图 D 是连通的,画出 D.

序、积集和 Kleene 闭包

14.54 设 $M=\{2,3,4,\cdots,\}$和 $M^2=M\times M$ 以如下方式排序:$(a,b)\precsim(c,d)$,如果 $a|c$ 且 $b\leqslant d$.
求 $M\times M$ 中所有极大和极小的元素.

14.55 设字母排序集 $A=\{a,b,c,\cdots,y,z\}$. Kleene 闭包 A^* 是 A 中所有字符串的集合. 设 L 是下列元素的集合:

gone, or, arm, go, an, about, gate, one, at, occur

(a) 将 L 按长度—字母序排列,即先按长度再按字母排列.

(b) 将 L 按字母排序排列.

14.56 设序集 A 和 B 分别如图 14-20(a)和(b)所示,
$S=A\times B$ 赋予积序,即:
$(a,b)\precsim(a',b')$,如果 $a\precsim a'$ 且 $b\precsim b'$.
填写正确的符号<,>或 ‖:

(a) $(4,b)$_____$(2,e)$.　　(b) $(3,a)$_____$(6,f)$.

(c) $(5,d)$_____$(1,a)$.　　(d) $(6,e)$_____$(2,b)$.

14.57 设常序集 $\mathbf{N}=\{1,2,3,\cdots\}$,$\mathbf{A}=\{a,b,c,\cdots,y,z\}$和字典排序集 $S=\mathbf{N}\times\mathbf{A}$. 将下列元素排列:
$(2,z),(1,c),(2,c),(1,y),(4,b),(4,z),(3,b),(2,a)$.

上界和下界　上确界和下确界

14.58 设序集 $S=\{a,b,c,d,e,f,g\}$,如图 14-14(a)所示. 设 $A=\{a,c,d\}$为 S 的子集

(a) 求 A 的上界集.　　(b) 求 A 的下界集.

(c) $\sup(A)$存在吗?　　(d) $\inf(A)$存在吗?

14.59 对于 S 的子集 $B=\{b,c,e\}$,重做问题 14.58.

14.60 设 $S=\{1,2,\cdots,7,8\}$,如图 14-14(b)所示,考虑 S 的子集 $A=\{3,6,7\}$.

(a) 求 A 的上界集.　　(b) 求 A 的下界集.

(c) $\sup(A)$存在吗?　　(d) $\inf(A)$存在吗?

14.61 对 S 的子集 $B=\{1,2,4,7\}$,回答问题 14.60.

14.62 考虑常序有理数集 $\mathbf{Q}$. 设 $A=\{x:x\in\mathbf{Q}$ 且 $5<x^3<27\}$.

(a) A 有上界或下界吗?

(b) $\sup(A)$或 $\inf(A)$存在吗?

14.63 考虑常序实数集 $\mathbf{R}$. 设 $A=\{x:x\in\mathbf{Q}$ 且 $5<x^3<27\}$.

(a) A 有上界或下界吗?

(b) $\sup(A)$或 $\inf(A)$存在吗?

同构序集　同构映射

14.64 设 S 为图 14-21(a)中的序集,假设 $A=\{1,2,3,4,5\}$与 S 同构,同构映射为:
$f=\{(a,1),(b,4),(c,5),(d,2),(e,3)\}$

画出 A 的 Hasse 图.

14.65 求具有 3 个元素 a,b,c 的非同构偏序集的个数.并画出它们的 Hasse 图.

14.66 求具有 4 个元素 a,b,c,d 的连通的非同构偏序集的个数.并画出它们的 Hasse 图.

14.67 求相似映射:$f:S\to S$ 的个数,S 是下面的有序集:(a) 图 14－20(a);(b) 图 14－20(b);(c) 图 14－20(c).

14.68 证明序集的同构关系 $A\simeq B$ 是一个等价关系,即:(a) 对于任何的序集 A,$A\simeq A$;(b) 若 $A\simeq B$,则 $B\simeq A$;(c)若 $A\simeq B$ 且 $B\simeq C$,则 $A\simeq C$.

良序集

14.69 假设 S 是 $A=\{a_1,a_2,a_3,\cdots\}$ $B=\{b_1,b_2,b_3,\cdots\}$ $C=\{c_1,c_2,c_3,\cdots\}$的并,排序如下

$S=\{A;B;C\}=\{a_1,a_2,\cdots,b_1,b_2,\cdots,c_1,c_2,\cdots\}$

(a) 证明 S 是良序的.

(b) 求 S 中所有的极限元素.

(c) 证明 S 与常序集 $\mathbf{N}=\{1,2,\cdots\}$不同构.

14.70 设序集 $A=\{a,b,c\}$,其中 $a<b<c$.设常序集 $\mathbf{N}=\{1,2,\cdots\}$.

(a) 证明 $S=\{A;\mathbf{N}\}$与 $\mathbf{N}$ 同构.

(b) 证明 $S'=\{\mathbf{N};A\}$与 $\mathbf{N}$ 非同构.

14.71 假设 A 是关系$\precsim$下的一个良序集,也是逆关系$\succsim$下的一个良序集,描述 A.

14.72 假设 A 和 B 是同构良序集,证明只有惟一的一个同构映射 $f:A\to B$.

14.73 设 S 为一个良序集,对于任何的 $a\in S$,集合 $S(a)=\{x:x<a\}$被称为 a 的前缀,证明 S 不能与它的一个前缀同构.(提示:用问题 14.30).

14.74 假设 $S(a)$和 $S(b)$是一个良序集 S 的两个不同的前缀,证明 $S(a)$和 $S(b)$不能同构.
(提示:用问题 14.73)

格

14.75 考虑图 14－22(a) 中的格 L.(a) 找出含有 5 个元素的所有子格.(b) 找出所有并不可约的元素和原子.(c) 若 a 和 b 的补元存在,请求出.(d) L 是分配格吗? L 是有补格吗?

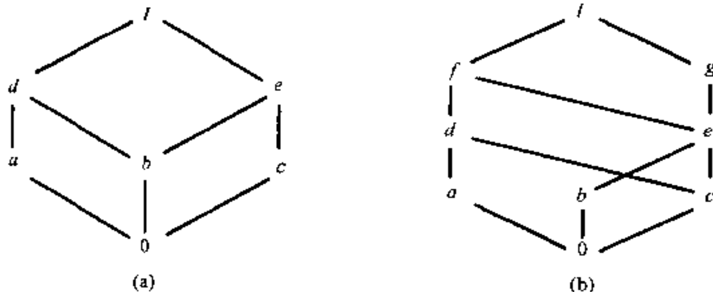


图 14－22

14.76 考虑如图 14－22(b)中的格,(a) 求并不可约元素.(b) 求原子.(c) 求 a 和 b 的补元,若它们存在的话.(d) 表达 M 中每个 x 成两两不可比的并不可约元素的并.(e) M 是分配格吗? M 是有补格吗?

14.77 考虑图 14－23(a)中的有界格 L.

(a) 若 a 和 f 的补元存在,请求出.

(b) 用尽可能多的方式,把 I 写成两两不可比的并不可约元素的并.

(c) L 是分配格吗?

(d) 描述 L 与自身的同构.

14.78 考虑图 14－23(b)中的有界格.

(a) 找出 a 和 c 的补元,如果存在的话.

(b) 用尽可能多的方式,把 I 写成两两不可比的并不可约元素的并.

(c) L 是分配格吗?

(d) 描述 L 的自同构.

14.79 考虑图 14-23(c)中的有界格 L.

(a) 求 a 和 c 的补元,如果存在的话.

(b) 用尽可能多的方式,把 I 写成两两不可比的并不可约元素的并.

(c) L 是分配格吗?

(d) 描述 L 的自同构.

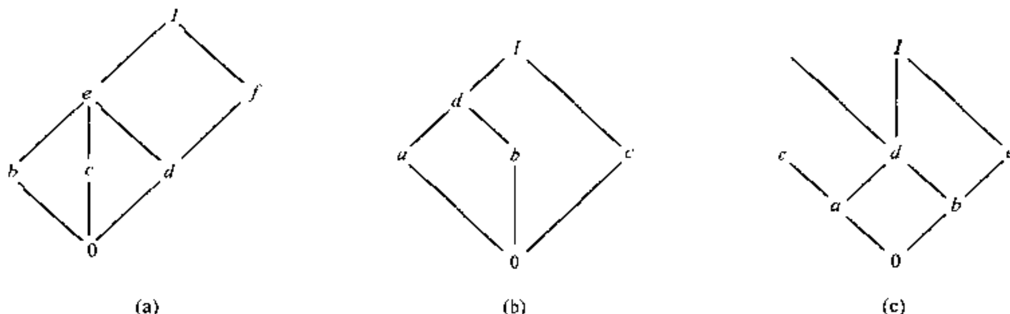


图 14-23

14.80 考虑格 $\mathbf{D}_{60}=\{1,2,3,4,5,6,10,12,15,20,30,60\}$,即 60 的因数在整除关系下序集.

(a) 画出 $\mathbf{D}_{60}$ 的 Hasse 图.

(b) 哪些元素是并不可约的? 哪些元素是原子?

(c) 若 2 和 10 的补元存在,请求出.

(d) 描述 L 到自身的同构.

14.81 考虑按照整除关系排序的正整数格 $\mathbf{N}$.

(a) 哪些元素是并不可约的.

(b) 哪些元素是原子?

14.82 证明下列"弱"的分配律对任何一个格都成立.

(a) $a\vee(b\wedge c)\leqslant(a\vee b)\wedge(a\vee c)$.

(b) $a\wedge(b\vee c)\geqslant(a\wedge b)\vee(a\wedge c)$.

14.83 设 $S=\{1,2,3,4\}$,用记号$[1,2,3,4]=[\{1,2\},\{3\},\{4\}]$. S 的三个划分是

$$P_1=[12,3,4],P_2=[12,34],P_3=[13,2,4].$$

(a) 找出 S 中另外 9 个划分.

(b) 设 L 是按照加细排序的 S 的 12 个划分构成的集合,即:$P_i\precsim P_j$,若 P_i 的每一块都是 P_j 的某一块的子集.例如 $P_1\precsim P_2$,但 P_2 与 P_3 是不可比的,证明 L 是有界格,画出它的 Hasse 图.

14.84 格 L 中的元素 a 是交不可约的,若 $a=x\wedge y$ 蕴含 $a=x$ 或 $a=y$,在下面格中找出所有交不可约的元素. (a)图 14-22(a). (b) 图 14-22(b). (c) $\mathbf{D}_{60}$(参照问题 14.80).

14.85 格 M 叫做模格,如果 $a\leqslant c$ 蕴含 $a\vee(b\wedge c)=(a\vee b)\wedge c$.

(a) 证明每个分配格是模格.

(b) 验证图 14-7(b)中的非分配格是模格,因此(a)的逆不真.

(c) 证明:14-7(a)中的非分配格是非模格.

(事实上,能够证明每一个非模格包含一个与图 14-7(a)同构的子格).

14.86 设 R 是一个环,L 是 R 中所有理想的集合.对于 R 中的理想 J,K,定义

$$J\vee K=J+K,J\wedge K=J\cap K.$$

证明 L 是一有界格.

补充题答案

14.40 (a) 极小元:4,6;极大元:1,2.

(b) 都没有.

(c) $\{1,3,4\},\{1,3,6\},\{2,3,4\},\{2,3,6\},\{2,5,6\}$.

14.41 (a) 极小元:d,f;极大元:a.

(b) 极小元:无;最大元:a.

(c) 有 11 个：$dfebca$, $dfecba$, $dfceba$, $fdebca$, $fdeba$, $fdceba$, $fedbca$, $fedcba$, $fcdeba$, $fecdba$, $fcedba$.

14.42 见图 14－24.

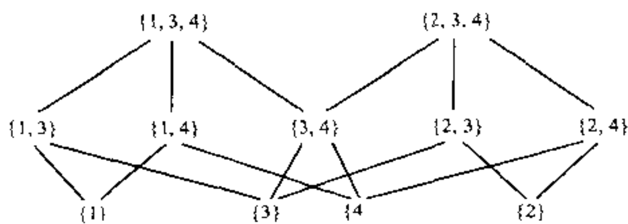


图 14－24

14.43 见图 14－25.

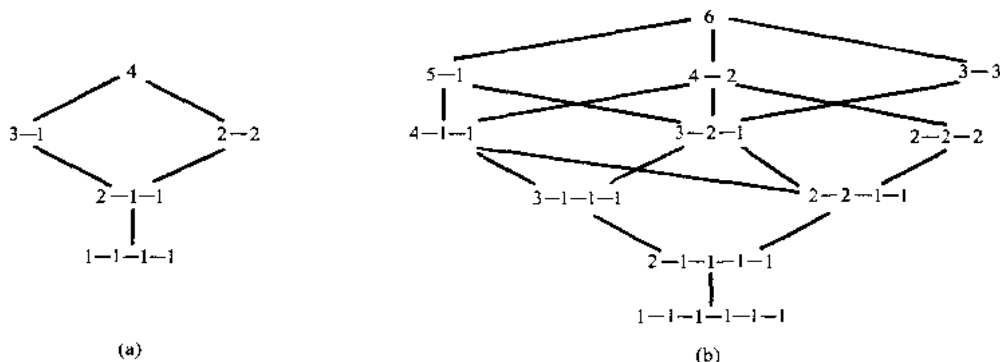


图 14－25

14.44 见图 14－26.

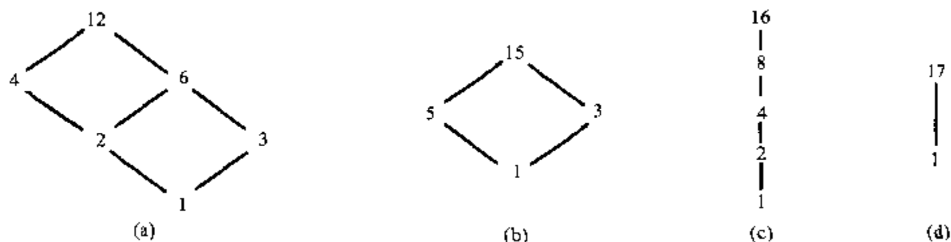


图 14－26

14.45 提示：画 S 的 Hasse 图.

(a) 极小元：e；极大元：a, d.

(b) 最小元：e；最大元：没有.

(c) $\{a, d\}$, $\{b, c\}$.

14.46 (a) 错. 例如：$\mathbf{N}\cup\{a\}$，其中 $1 \ll a$ 和 $\mathbf{N}$ 按≤排序.

(b) 正确.

(c) 正确.

14.47 (a) 极小元：a；极大元：d, e.

(b) 最小元：a；最大元：没有.

(c) 任何包含 c 略去 a 的子集，即 c, cb, cd, ce, cbd, cbe, cde, $abde$.

(d) c, cd, ce, cde.

(e) abd, , acd, ace.

14.48 (a) 极小元：a, b；极大元：e, f.

(b) 最小元：没有；最大元：没有.

(c) ace, acf, bce, bcf, bdf.

14.49 (a) 4. (b) 没有.

14.50 (a) 6. (b) 没有.

14.51 $abcde, abced, acbde, acbed, acebd$.

14.52 11.

14.53 $a \ll b, a \ll c, c \ll d$.

14.54 极小元:$(p,2)$其中 p 是一个素数,无极大元.

14.55 (a) an, at, go, or, arm, one, gate, gone, about, occur.

(b) an, about, arm, at, gate, go, gone, occur, one, or.

14.56 (a) ∥; (b) $>$; (c) ∥; (d) $<$.

14.57 $1c, 1y, 2a, 2c, 2z, 3b, 4b, 4z$.

14.58 (a) e, f, g; (b) a; (c) $\sup(A) = e$; (d) $\inf(A) = a$.

14.59 (a) e, f, g; (b) 无; (c) $\sup(B) = e$; (d) 无.

14.60 (a) 1,2,3. (b) 8. (c) $\sup(A) = 3$. (d) $\inf(A) = 8$.

14.61 (a) 无; (b) 8; (c) 无; (d) $\inf(B) = 8$.

14.62 (a) 两者都是; (b) $\sup(A) = 3$, $\inf(A)$ 不存在.

14.63 (a) 两者都是; (b) $\sup(A) = 3, \inf(A) = \sqrt[3]{5}$.

14.64 见图 14-27.

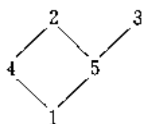


图 14-27

14.65 4 种: (1) a, b, c; (2) $a, b \ll c$; (3) $a \ll b, a \ll c$; (4) $a \ll b \ll c$.

14.66 四种,见图 14-28.

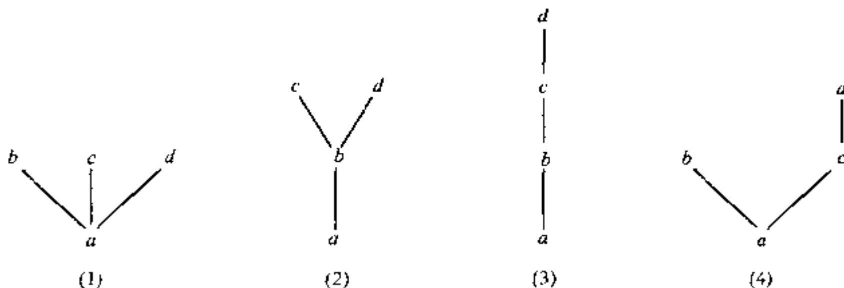


图 14-28

14.67 (a) 1,恒等映射. (b) 1. (c) 2.

14.69 (b) b_1, c_1. (c) **N** 没有极限点.

14.70 (a) 通过 $f(a) = 1, f(b) = 2, f(3) = 3, f(n) = n + 3$ 定义 $f: S \to \mathbf{N}$

(b) 元素 a 是 S' 的一个极限点,但 **N** 没有极限点.

14.71 A 是有限线性序集.

14.75 (a) 六种: $0abcdI, 0acdI, 0adeI, 0bceI, 0aceI, 0cdeI$.

(b) (i) $a, b, e, 0$; (ii) a, b, c.

(c) c, e 是 a 的补元, b 没有补元.

(d) 不,不.

14.76 (a) $a, b, c, g, 0$. (b) a, b, c.

(c) $a; g; b$; 无.

(d) $I = a \vee g, f = a \vee b = a \vee c, e = b \vee c, d = a \vee c$

其他元素是并不可约的.

(e) 不,不.

14.77 (a) e 没有, f 有 b 和 c.

(b) $I = c \vee d \vee f = b \vee c \vee f = b \vee d \vee f$.

(c) 不,因为分解式不惟一.

(d) 两种:0,d,e,f,I 必须映射到自身. 因此 $F=1_L$,L 上恒等映射或 $F=\{(b,c),(c,b)\}$.

14.78 (a) a 有 c,c 有 a 和 b.

(b) $I=a\vee c=b\vee c$.

(c) 不.

(d) 两种:0,c,d,I 必须映射到自身,因此 $f=1_L$ 或 $f=\{(a,b),(b,a)\}$.

14.79 (a)a 有 e,c 有 b 和 e.

(b)$I=a\vee e=b\vee c=c\vee e$.

(c)不是.

(d)两种:0,d,I 映射到自身,因此 $f=1_L$ 或 $f=\{(a,b),(b,a),(c,d),(d,c)\}$.

14.80 (a) 见图 14-29. (b) 1,2,3,4,5,原子是 2,3,5.

(c) 2 没有,10 有 3.

(d) $60=4\vee 3\vee 5$,$30=2\vee 3\vee 5$,$20=4\vee 5$,

$15=3\vee 5$,$12=3\vee 4$,$10=2\vee 5$,$6=2\vee 3$.

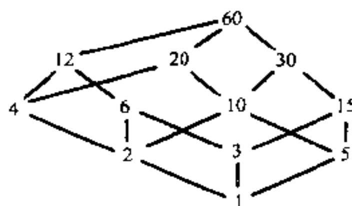


图 14-29

14.81 (a) 素数的幂和 1. (b)素数.

14.83 (a) [1,2,3,4],[14,2,3],[13,24],[14,23],

[123,4],[124,3],[134,2],[234,1],[1234].

(b) 见图 14-30.

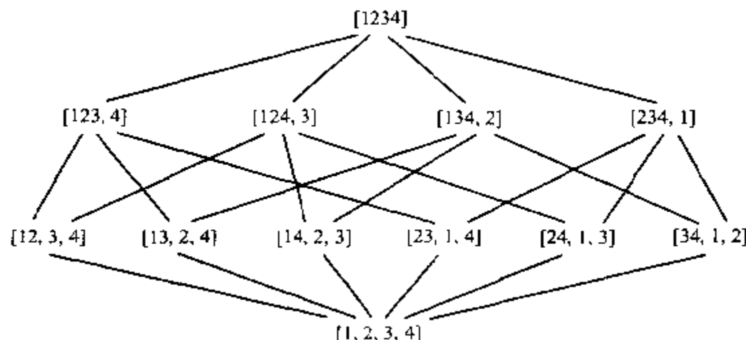


图 14-30

14.84 从几何意义下,一个元素 $a\neq I$ 是交不可约的,当且仅当 a 只有一个直接继元,

(a) a,c,d,e,I. (b) a,b,d,f,g,I.

(c) 4,6,10,12,15,60.

14.85 (a) 若 $a\leqslant c$,则 $a\vee c=c$.

因此

$$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)=(a\vee b)\wedge c.$$

(c) 这里 $a\leqslant c$,但 $a\vee(b\wedge c)=a\vee 0=a$ 和$(a\vee b)\wedge c=I\wedge c=c$;因此

$$a\vee(b\wedge c)\neq(a\vee b)\wedge c.$$

第十五章 布尔代数

15.1 引 言

集合和命题都满足相似的法则，我们已在表 1-1 和表 4-1（分别在第一章和第四章）中列出. 这些法则被用于定义一种抽象的数学结构，叫做布尔代数. 这是以数学家 George Boole (1813～1864) 命名的.

15.2 基本定义

设 B 是一个非空集合，具有二元运算 $+$ 和 $*$，一元运算 $'$ 和两个不同的元素 0, 1. 称 B 为一个布尔代数，若对任意的 $a,b,c\in B$，以下公理满足.

[$\mathbf{B}_1$] 交换律

(1a) $a+b=b+a$；(1b) $a*b=b*a$.

[$\mathbf{B}_2$] 分配律

(2a) $a+(b*c)=(a+b)*(a+c)$；

(2b) $a*(b+c)=(a*b)+(a*c)$.

[$\mathbf{B}_3$] 单位元律

(3a) $a+0=a$；(3b) $a*1=a$.

[$\mathbf{B}_4$] 互补律

(4a) $a+a'=1$；(4b) $a*a'=0$.

有时，当我们要强调其六个部分时，用 $(B,+,*,',0,1)$ 来表示一个布尔代数. 称 0 为零元素，1 为单位元素，a' 为 a 的补. 通常，我们省略符号 $*$. 这样，(2b) 就可以写成 $a(b+c)=ab+ac$，这是环和域里熟悉的恒等式. 但是，(2a) 写成 $a+bc=(a+b)(a+c)$，这与普通代数中的分配律不同.

运算 $+$，$*$ 与 $'$ 分别称为和，积与补. 如果没有括号的话，则可采用习惯的方法. $'$ 运算优先于 $*$ 运算，$*$ 运算优先于 $+$ 运算. 例如，

$a+b*c$ 表示 $a+(b*c)$ 而不是 $(a+b)*c$，

$a*b'$ 表示 $a*(b')$ 而不是 $(a*b)'$.

当然，当 $a+b*c$ 写成 $a+bc$ 时，其意思是清楚的.

例 15.1 (a) 假设 $B=\{0,1\}$ 是一个位元（二元数码）的集合，具有二元运算 $+$ 和 $*$，一元运算 $'$，如图15-1定义. 这样 B 就是一个布尔代数.（注：$'$ 的简单运算是：$1'=0, 0'=1$）.

+	1	0
1	1	1
0	1	0

*	1	0
1	1	0
0	0	0

'	1	0
	0	1

图 15-1

(b) 设 $B^n=B\times B\times\cdots\times B$（$n$ 个因子），运算 $+$，$*$ 和 $'$ 用各个分量定义，见图 15-1. 为了方便起见，我们把 B^n 的元素写成没有逗号的 n 位位元序列. 例如，$x=110011$，$y=111000$，这都属于 B^6. 因此

$$x+y=111011, x*y=110000, x'=001100.$$

这样 B^n 就是一个布尔代数. 这里 $0=000\cdots0$ 是零元素，$1=111\cdots1$ 是单位元素. 我们注意到 B^n 有 2^n 个元素.

(c) 设 $\mathbf{D}_{70}=\{1,2,5,7,10,14,35,70\}$，其中的元素都是 70 的因数. 在 $\mathbf{D}_{70}$ 上定义 $+$，

$*$ 和 $'$：

$$a+b=\mathrm{lcm}(a,b),a*b=\gcd(a,b),a'=\frac{70}{a}.$$

这样 $\mathbf{D}_{70}$ 是一个布尔代数，具有零元素 1 和单位元素 70.

(d) 设 C 是一个集簇，对于集合运算的并、交、补都是封闭的. 这样 C 就是一个布尔代数，具有空集 $\varnothing$ 作为零元素，全集 U 作为单位元素.

子代数，同构的布尔代数

设 C 是布尔代数 B 的一个非空子集. 如果 C 本身是布尔代数(相对于 B 的运算)，我们就称 C 是 B 的一个子代数. 注意 C 是 B 的一个子代数当且仅当 C 对于 B 中的三种运算，如 $+$，$*$ 和 $'$ 都是封闭的. 例如，$\{1,2,35,70\}$ 是例 15.1(c) 中 $\mathbf{D}_{70}$ 的一个子代数.

两个布尔代数 B 和 B' 称为同构的，如果有一一对应(双射) $f:B\to B'$，并保持这三种运算，即，使得对于 B 中的任意元素 a 和 b，有

$$f(a+b)=f(a)+f(b),f(a*b)=f(a)*f(b) \text{和} f(a')=f(a)'.$$

15.3 对偶性

在布尔代数中，任意命题的对偶是由在原命题中交换运算 $+$ 和 $*$，并交换单位元 0 和 1 得到的命题. 例如：

$$(1+a)*(b+0)=b \text{ 的对偶命题就是} (0*a)+(b*1)=b.$$

显然布尔代数 B 的公理是对称的. 即，B 的公理集的对偶与原公理集是相同的. 因此，在 B 中成立重要的对偶原理，即，

定理 15.1 (对偶原理) 任何布尔代数的真命题的对偶仍是真命题.

换句话说，如果一个命题是布尔代数公理的结论，那么对偶命题仍是那些公理的结论，因为只要把原来命题的证明的每一步换成对偶形式即能证明对偶命题.

15.4 基本定理

由公理 $[\mathbf{B}_1]\sim[\mathbf{B}_4]$，可证明(问题 15.5)下列定理.

定理 15.2 设 a,b,c 是布尔代数 B 中的任意元素.

(i) 幂等律：

(5a) $a+a=a$；(5b) $a*a=a$.

(ii) 有界律：

(6a) $a+1=1$；(6b) $a*0=0$.

(iii) 吸收律：

(7a) $a+(a*b)=a$；(7b) $a*(a+b)=a$.

(iv) 结合律：

(8a) $(a+b)+c=a+(b+c)$；(8b) $(a*b)*c=a*(b*c)$.

定理 15.2 和我们的公理仍不能包含表 1-1 中所列出的集合的性质. 下面的两条定理将给出其余的性质.

定理 15.3 设 a 是布尔代数 B 中的任意元素.

(i) (补的惟一性)　如果 $a+x=1$ 且 $a*x=0$，那么 $x=a'$.

(ii) (对合律) $(a')'=a$.

(iii) (9a) $0'=1$；(9b) $1'=0$.

定理 15.4 (DeMorgan 律) (10a) $(a+b)'=a'*b'$；(10b) $(a*b)'=a'+b'$.

这些定理将在问题 15.6 和 15.7 中证明.

15.5 作为格的布尔代数

根据定理 15.2 和公理 $[\mathbf{B}_1]$，每个布尔代数都满足结合律，交换律和吸收律，因此它是一个

格，并且+和 * 处分别为∨和∧运算. 相对于这个格，对于任意元素 $a\in B$，$a+1=1$ 蕴含 $a\leqslant 1$，而 $a*0=0$ 蕴含 $0\leqslant a$. 于是，B 是一个有界格. 进一步，公理[$\mathbf{B}_2$]和[$\mathbf{B}_4$]表明 B 也是分配格和有补格. 反之，每个有界的，分配的，有补的格 L 满足公理[$\mathbf{B}_1$]~[$\mathbf{B}_4$]. 因此，我们有下列定义

替换定义 一个布尔代数 B 是一个有界的，分配的，有补的格.

既然布尔代数 B 是一个格，它就有自然的偏序关系(所以能够作出它的 Hasse 图). 当等价条件 $a+b=b$ 且 $a*b=a$ 满足时，我们定义 $a\leqslant b$. 在布尔代数中，我们实际上能给出更多的等价条件.

定理 15.5 在布尔代数中，下列条件是等价的：

(1) $a+b=b$　　(2) $a*b=a$

(3) $a'+b=1$　　(4) $a*b'=0$.

这样，在布尔代数中，只要知道上列四个条件之一是正确的话，我们就可以写 $a\leqslant b$.

例 15.2 (a) 考虑一个集簇上的布尔代数. 如果 A 是 B 的一个子集，那么 A 先于 B. 定理 15.4 表明如果 $A\subseteq B$，(如图 15-2)，那么以下等式成立：

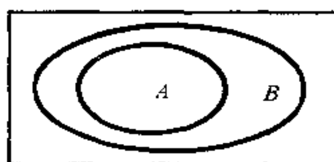
(1) $A\cup B=B$　　(2) $A\cap B=A$

(3) $A^c\cup B=U$　　(4) $A\cap B^c=\varnothing$.

(b) 考虑布尔代数 $\mathbf{D}_{70}$. 如果 a 整除 b，那么 a 先于 b. 在这个例子中，$\mathrm{lcm}(a,b)=b$，$\gcd(a,b)=a$. 例如，令 $a=2$，$b=14$，那么下列等式成立：

(1) $\mathrm{lcm}(2,14)=14$　　(2) $\gcd(2,14)=2$

(3) $\mathrm{lcm}(2',14)=\mathrm{lcm}(35,14)=70$　　(4) $\gcd(2,14')=\gcd(2,5)=1$.



A 是 B 的一个子集

图 15-2

15.6 表示定理

假设 B 是一个有限的布尔代数. 回忆(14.9 节)B 中的元素 a 是一个原子，如果 a 直接跟着 0，也就是说，如果 $0\ll a$. 设 A 是 B 的原子的集合且 $P(A)$ 是原子集 A 的所有子集的布尔代数. 由定理 14.8，B 中每一个 $x\neq 0$ 都可以惟一表示成(除了顺序)原子的和(并)，即 A 中的元素的和(并). 比如，

$$x=a_1+a_2+\cdots+a_r$$

是这样的一个表示. 考虑函数 $f:B\to P(A)$，这里

$$f(x)=\{a_1,a_2,\cdots,a_r\}.$$

这种映射是良好定义的，因为表示方法是惟一的.

定理 15.6 上面的映射 $f:B\to P(A)$ 是一个同构映射.

由此可见集合论与抽象布尔代数之间的本质联系，每一个有限布尔代数在结构上与一个集簇上的布尔代数是相同的.

如果集合 A 有 n 个元素，那么它的幂集 $P(A)$ 就有 2^n 个元素. 同此，由上述定理 15.6 可得到下列结论.

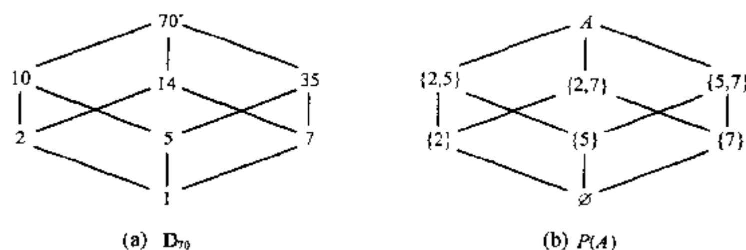
推论 15.7 一个有限的布尔代数有 2^n 个元素，n 为正整数.

例 15.3 考虑布尔代数 $\mathbf{D}_{70}=\{1,2,5,\cdots,70\}$，如图 15-3(a). 注意 $A=\{2,5,7\}$ 是 $\mathbf{D}_{70}$ 的原子的集合. 我们用原子惟一表示每个非原子：

$$10=2\vee 5, 14=2\vee 7, 35=5\vee 7, 70=2\vee 5\vee 7.$$

图 15-3(b)给出原子集 A 的幂集 $P(A)$ 的布尔代数的 Hasse 图. 显然这两幅图在结

构上是相同的.



(a) $\mathbf{D}_{70}$　　(b) $P(A)$

图 15 - 3

15.7　集合的积和式

本节通过集合论的一个例子来引出布尔代数中积和式的概念. 考虑图 15 - 4 中的三个集合 A,B 和 C. 观察这些集合划分矩形(全集)为八个小块,表示如下:

(1) $A\cap B\cap C$,　(2) $A\cap B\cap C^c$,　(3) $A\cap B^c\cap C$,　(4) $A^c\cap B\cap C$,

(5) $A\cap B^c\cap C^c$,　(6) $A^c\cap B\cap C^c$,　(7) $A^c\cap B^c\cap C$,　(8) $A^c\cap B^c\cap C^c$.

这八个集合的每一个都是由 $A^*\cap B^*\cap C^*$ 的形式构成的,这里

$$A^*=A\text{ 或 }A^c,B^*=B\text{ 或 }B^c,C^*=C\text{ 或 }C^c.$$

考虑任何一个由 A,B,C 表示的非空集合 E. 比如:

$$E=[(A\cap B^c)^c\cup(A^c\cap C^c)]\cap[(B^c\cup C)^c\cap(A\cup C^c)].$$

这样 E 就代表了图 15 - 4 中的某一块. 因此,E 将惟一表示成八个集合中的一个或多个的并集.

假设我们将并作为和,交作为积. 这样,上列的八个集合就是积,而 E 惟一表达式就是一个积的和(并). 这种 E 的惟一的表达式与下面将要讨论的布尔代数的完全的积和式 E 是相同的.

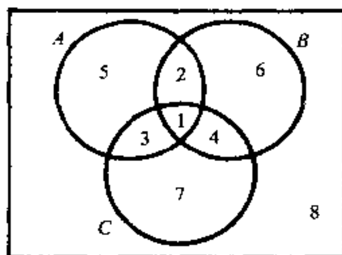


图 15 - 4

15.8　布尔代数的积和式

考虑一个变元(字母或符号)的集合,比如 $x_1,x_2,\cdots,x_n$.

由这些变元构成的布尔表达式 E 有时写作 $E(x_1,x_2,\cdots,x_n)$,是一个变元或这些变元通过布尔运算 $+$, $*$ 和 $'$ 构成的式子. (一般地,表达式 E 必须是良好构成的,即 $+$ 和 $*$ 用于二元运算, $'$ 用于一元运算.) 例如

$$E_1=(x+y'z)'+(xyz'+x'y)'\text{ 和 }E_2=((xy'z'+y)'+x'z)'$$

是关于 x,y,z 的布尔表达式.

一个文字是一个变元或变元的补. 例如 x,x',y,y' 等等. 一个基本积是一个文字,或两个或多个文字组成的积,在这个积中没有两个文字包含同一个变元. 因此,$xz',xy'z,x,y',x'yz$ 是基本积,但是 $xyx'z$ 和 $xyzy$ 不是. 注意,任何文字的乘积可以简化为 0 或者一个基本积. 例如 $xyx'z=0$,因为 $xx'=0$(互补律);$xyzy=xyz$,因为 $yy=y$(幂等律).

如果基本积 P_1 中的文字也是基本积 P_2 中的文字,那么称 P_1 被包含在 P_2 之中. 例如: $x'z$ 包含在 $x'yz$ 中,但是 $x'z$ 不包含在 $xy'z$ 中,因为 x' 不是 $xy'z$ 中的文字. 经观察,如果 P_1 包含在 P_2 中,就说 $P_2=P_1*Q$,根据吸收律,

$$P_1+P_2=P_1+P_1*Q=P_1$$

于是有例子

$$x'z+x'yz=x'z.$$

定义　若布尔表达式 E 是一个基本积或是两个或更多基本积的和,且这些积是互不包含的,这样的一个布尔表达式 E 称为积和表达式.

定义　设 E 是任意的布尔表达式. E 的一个积和式是一个等价的布尔积和表达式.

例 15.4　考虑表达式

$$E_1=xz'+y'z+xyz', E_2=xz'+x'yz'+xy'z.$$

虽然第一个表达式 E_1 是积的和，但是它不是积和表达式. 特别地，积 xz' 包含在积 xyz' 中. 但是，根据吸收律，E_1 可以表达为

$$E_1=xz'+y'z+xyz'=xz'+xyz'+y'z=xz'+y'z.$$

这是 E_1 的积和表达式. 第二个表达式 E_2 已经是积和表达式.

求积和表达式的算法

下面的四步算法是应用布尔代数的定律将任一布尔表达式 E 化为一个等价的积和表达式.

算法 15.8A　输入一个布尔表达式 E. 输出一个与 E 等价的积和表达式.

步骤 1　应用 DeMorgan 律和对合律把补运算放到括号里面去，直到最后补运算仅仅出现在变元上. 那么，E 就仅由文字的积与和组成.

步骤 2　利用分配律把 E 变为积的和.

步骤 3　利用交换律，幂等律和互补律把 E 中的每一个积变为 0 或一个基本积.

步骤 4　利用吸收律和单位元律把 E 变为一个积和表达式.

例 15.5　算法 15.8A 用于下列的布尔表达式

$$E=((xy)'z)'((x'+z)(y'+z'))'.$$

步骤 1　由 DeMorgan 律和对合律，得

$$E=((xy)''+z')((x'+z)'+(y'+z')')=(xy-z')(xz'+yz).$$

现在 E 只是由文字的和与积组成.

步骤 2　由分配律，得

$$E=xyxz'+xyyz+xz'z'+yzz'.$$

现在 E 是积的和.

步骤 3　由交换律，幂等律及互补律，得

$$E=xyz'+xyz+xz'+0.$$

E 中的每一项都是基本的积或 0.

步骤 4　积 ac' 包含在 abc'. 因此，根据吸收律，有

$$xz'+(xz'*y)=xz'.$$

因此，我们可以从和中删除 abc'，并由单位元律，从和中删除 0. 由此，

$$E=xyz+xz'.$$

现在 E 是积和表达式.

完全积和式

一个布尔表达式 $E=E(x_1,x_2,\cdots,x_n)$ 是一个*完全积和表达式*，若 E 是一个积和表达式，并且每个积 P 包括了所有的 n 个变元. 如此的一个基本积 P 被称为*极小项*. 对于 n 个变元，如此的积共有 2^n 个.

定理 15.8　每个非零的布尔表达式 $E=E(x_1,x_2,\cdots,x_n)$ 等价于惟一的完全积和表达式.

上面关于 E 的惟一的表达式被称为 E 的*完全积和式*. 回忆算法 15.8A 我们知道如何转变 E 为一个积和式. 下面的算法给出将积和式化为完全积和式的方法.

算法 15.8B　输入一个布尔积和表达式 $E=E(x_1,x_2,\cdots,x_n)$. 输出一个与 E 等价的完全积和表达式.

步骤 1　找出 E 中不包括变量 x_i 的积 P，然后以 x_i+x_i' 乘 P，删除重复的积.（这是可能的，因为 $x_i+x_i'=1$，还有 $P+P=P$).

步骤 2　重复步骤 1，直到 E 中每一个积 P 都是极小项，即每个积 P 包括所有的变元.

例 15.6　用完全积和式表示 $E(x,y,z)=x(y'z)'$.

(a) 算法 15.8A 用于 E 得

$$E=x(y'z)'=x(y+z')=xy+xz'.$$

现在 E 是积和表达式.

(b) 算法 15.8B，用于 E 得

$$\begin{aligned}E&=xy(z+z')+xz'(y+y')=xyz+xyz'+xyz'+xy'z'\\&=xyz+xyz'+xy'z'.\end{aligned}$$

现在 E 是完全积和式.

注　这一章节的术语还不是标准的. 布尔表达式 E 的积和式也叫做 E 的*分离正规式*或 DNF，E 的完全积和式也叫做 E 的*完全分离正规式*或是 E 的*极小项标准式*.

15.9　极小布尔表达式，素隐项

有许多方法可以表示同一个布尔表达式 E. 这里我们定义并研究 E 的极小的积和式. 还要定义并研究 E 的素隐项. 因为极小的积和式涉及到素隐项. 其余极小式也存在，但它们的研究已超出了本书的范围.

极小的积和式

考虑一个布尔积和表达式 E. 设 E_L 表示 E 中文字的数目（重复计数），设 E_S 表示 E 中和项的数目. 例如，假设

$$E=xyz'+x'y't+xy'z't+x'yzt.$$

那么

$$E_L=3+3+4+4=14, E_S=4.$$

假设 E 和 F 是等价的布尔积和表达式. 我们就说 E 比 F *简洁*，若

(i) $E_L<F_L$ 且 $E_S\leqslant F_L$　或(ii) $E_L\leqslant F_L$ 且 $E_S<F_L$，我们说 E 是*极小的*，如果没有比 E 简洁的等价的积和表达式. 注意可能有不止一种等价的极小积和表达式.

素隐项

一个基本积 P 被称作一个布尔表达式 E 的*素隐项*，若

$$P+E=E.$$

且 P 中不包含具备这个性质的其他基本积. 例如，假设

$$E=xy'+xyz'+x'yz',$$

我们能（问题 15.15）证明

$$xz'+E=E \text{ 但 } x+E\neq E \text{ 且 } z'+E\neq E.$$

因此 xz' 是 E 的一个素隐项.

定理 15.9　一个布尔表达式 E 的极小的积和表达式是 E 的素隐项的和.

下面基于基本积的共识给出一种求 E 的素隐项的方法. 这种方法以后可以被用作求 E 的极小积和式. 15.12 节将给出求素隐项的几何方法.

基本积的共识

设 P_1 和 P_2 是两个基本积，而且恰好有一个变元，如 x_k，其非补形式出现在一个积中，补的形式出现在另一个积中. 那么 P_1 和 P_2 的共识是在 x_k 和 x'_k 删除后的文字 P_1 和文字 P_2 的积(没有重复).（我们没有定义 $P_1=x$ 和 $P_2=x'$ 的共识）.

我们有下面的引理(在问题 15.19 中证明).

引理 15.10 假设 Q 是 P_1 和 P_2 的共识，那么，

$$P_1+P_2+Q=P_1+P_2.$$

例 15.7 求下列 P_1 和 P_2 的共识：

(a) $P_1=xyz's, P_2=xy't$.

删除 y 和 y'，然后把 P_1 和 P_2 的文字相乘(不重复)就得到 $Q=xz'st$.

(b) $P_1=xy', P_2=y$.

删除 y 和 y'，结果是 $Q=x$.

(c) $P_1=x'yz, P_2=x'yt$.

没有变元出现在一个积中，且它的补出现在另一个积中. 因此，P_1 和 P_2 不具有共识.

(d) $P_1=x'yz, P_2=xyz'$.

因为 x 和 z 两个变元分别以非补形式出现在一个积中，以补形式出现在另一积中，所以 P_1 和 P_2 没有共识.

用共识方法求素隐项

下面的算法，叫做共识方法，用于求布尔表达式的素隐项.

> **算法 15.9A (共识方法)** 输入一个布尔表达式 $E=P_1+P_2+\cdots+P_m$，这里 P_S 是基本积. 输出表达式 E，以它的素隐项的和的形式.（定理 15.11）
>
> **第一步** 若基本积 P_i 中包含其他基本积 P_j，那么就把 P_i 删除.
>
> **第二步** 增加 P_i 和 P_j 的共识 Q，如果 Q 不包含任何 P_S.（根据引理 15.10，这是允许的.）
>
> **第三步** 重复第一步与第二步，直到第一步、第二步不能用为止.

下面的定理给出了上面算法的基本性质.

定理 15.11 共识方法最终会停止，因而 E 由它的素隐项的和表示.

例 15.8 设 $E=xyz+x'z'+xyz'+x'y'z+x'yz'$，那么

$$\begin{aligned}
E &= xyz+x'z'+xyz'+x'y'z && (x'yz' \text{包含 } x'z')\\
&= xyz+x'y'+xyz'+x'y'z+xy && (xyz \text{ 和 } xyz' \text{的共识})\\
&= x'z'+x'y'z+xy && (xyz \text{ 和 } xyz' \text{包含 } xy)\\
&= x'z'+x'y'z+xy+x'y' && (x'z' \text{和 } x'y'z \text{ 的共识})\\
&= x'z'+xy+x'y' && (x'y'z \text{ 包含 } x'y')\\
&= x'z'+xy+x'y'+yz'. && (x'z' \text{和 } xy \text{ 的共识})
\end{aligned}$$

现在，共识方法中的每一步都不能改变 E. 因此 E 是它的素隐项的和，这个和出现在最后一行，即 $x'z'$，xy，$x'y'$ 和 yz'.

求极小积和式

共识方法(算法 15.9A)可以用来把一个布尔表达式 E 表示为它的素隐项的和. 下面用这种和找出 E 的一个极小积和式.

算法 15.9B　输入一个布尔表达式 $E=P_1+P_2+\cdots+P_m$，这里 P_S 是所有 E 的素隐项. 输出 E 的极小积和表达式.

第一步　表达每个素隐项 P 作为一个完全积和式.

第二步　一个个地删除那些素隐项，它们的和项出现在其他素隐项的和项中.

例 15.9　我们应用算法15.9B 于

$$E=x'z'+xy+x'y'+yz'.$$

(根据例 15.8，E 现在表达成它的所有素隐项的和.)

第一步　把 E 的每个素隐项表达成一个完全积和式，得到

$$x'z'=x'z'(y+y')=x'yz'+x'y'z',$$
$$xy=xy(z+z')=xyz+xyz',$$
$$x'y'=x'y'(z+z')=x'y'z+x'y'z',$$
$$yz'=yz'(x+x')=xyz'+x'yz'.$$

第二步　$x'z'$ 的和项是 $x'yz$ 和 $x'y'z'$，它们出现在其他的和项中. 因此，去掉 $x'z'$ 得到

$$E=xy+x'y'+yz'$$

没有其他素隐项的和项出现在剩下的素隐项的和项之中，因此这是 E 的一个极小积和式. 换句话说，没有其他素隐项是多余的，即如果保持 E 不变，没有其他素隐项是可以去掉的.

15.10　逻辑门与电路

逻辑电路(也叫做*逻辑网*)是由某种被叫做逻辑门的基本电路构成的. 每个逻辑电路可以看作是一台机器 L，L 包含一个或多个输入装置和惟一的输出装置. L 中的每个输入装置送出信号，具体地说，一个*位元*(二进制数)

0 或 1

对于电路 L，L 处理位元集产生输出位元. 于是一个 n-位元序列可以被分配到每个输入装置，且 L 处理这些输入序列，每次一个位元，产生一个 n-位元的输出序列. 首先我们定义逻辑门，然后再研究逻辑电路.

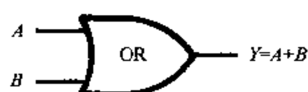
逻辑门

下面描述三种基本的逻辑门. 我们采用惯例，那些从左边进入门符的线是输入线. 右边的单线是输出线.

(a) **或门**　图 15-5(a)表示一个输入为 A 和 B，输出为 $Y=A+B$ 的或门，这里"加法"由图15-5(b)中的"值表"定义. 因此输出 $Y=0$ 当且仅当输入 $A=0$ 且 $B=0$. 这种或门可有多于两个的输入. 图 15-5(c)表示一个有四个输入 A,B,C,D 的或门，输出 $Y=A+B+C+D$. 只有当所有输入都为零时，输出 $Y=0$.

例如，假设图 15-5(c)中输入数据是下面的 8-位元序列：

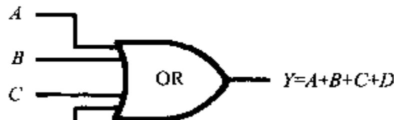
$$A=10000101,B=10100001,C=00100100,D=10010101.$$



(a) 或门

A	B	A+B
1	1	1
1	0	1
0	1	1
0	0	0

(b)



(c)

图 15-5

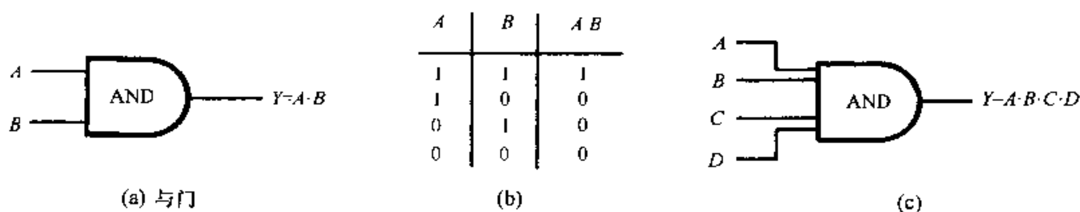
当所有的输入位元为 0 时，或门输出为 0. 这只发生在第二个，第五个及第七个位置（从左至右读）. 因此输出序列 $Y=10110101$.

（b）**与门**　图 15－6(a)表示一个输入为 A 和 B，输出为 $Y=A\cdot B$（或简记 $Y=AB$）的与门，这里“乘法”由图 15－6(b)中的“值表”定义. 因此当输入 $A=1$ 且 $B=1$ 时，输出 $Y=1$；否则 $Y=0$. 这种与门可有多于两个输入. 图 15－6(c)表示一个与门有 4 个输入 A,B,C,D，输出 $Y=A\cdot B\cdot C\cdot D$. 输出 $Y=1$ 当且仅当所有输入均为 1.

例如，假设图 15－6(c)中的输入数据是下面的 8－位元的序列：

$$A=11100111, B=01111011, C=01110011, D=11101110.$$

当所有输入位元为 1 时，与门输出为 1. 这只发生在第二个，第三个，第七个位置. 因此，输出序列是 $Y=01100010$.

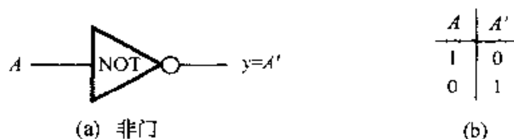


A	B	A B
1	1	1
1	0	0
0	1	0
0	0	0

(a) 与门　　　(b)　　　(c)

图 15－6

（c）**非门**　图 15－7(a)表示一个非门，也叫做一个颠倒，有输入 A 和输出 $Y=A'$. 这里“颠倒”，用撇点表示且由图 15－7(b)中的“值表”定义. 输出 $Y=A'$的值是输入 A 的相反值；也就是当 $A=0$ 时 $A'=1$；当 $A=1$ 时 $A'=0$. 我们强调一个非门只能有一个输入，而或门和与门可有两个或更多的输入.



A	A'
1	0
0	1

(a) 非门　　　(b)

图 15－7

例如，假定一个非门处理下列三个序列：

$$A_1=110001, A_2=10001111, A_3=101100111000.$$

非门将 0 变为 1，将 1 变为 0. 因此，

$$A'_1=001110, A_2=01110000, A_3=010011000111$$

就是三个相应的输出.

逻辑电路

逻辑电路 L 是一个良好形成的结构，它的基本元件是上述的或门、与门和非门. 图 15－8 是有输入 A,B,C 和输出 Y 的逻辑电路的例子. 标注黑点的位置表示在该处输入线分开使得位元信号被发向不止一个方向.（通常，为方便计，我们将省略门符号内部的字母.）从左到右运算，我们以输入 A,B,C 的术语表达 Y 如下. 与门的输出是 $A\cdot B$，它接下去被否认生成$(A\cdot B)'$. 较低的或门输出 $A'-C$，它接下去被否认生成$(A'+C)'$. 右边的或门，输入是$(A\cdot B)'$和

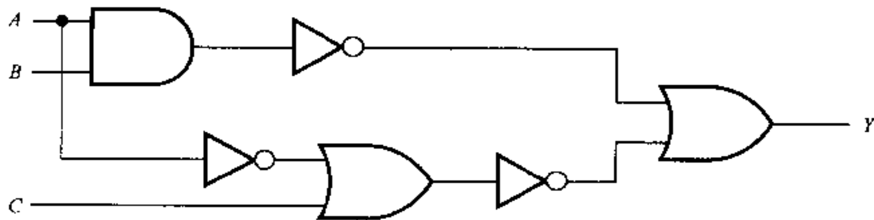


图 15－8

$(A'+C)'$，输出即为所需表达式.

$$Y=(A\cdot B)'+(A'+C)'.$$

逻辑电路与布尔代数

容易看出或门、与门和非门的值表与各自的命题 $p\vee q$（析取，"p 或 q"），$p\wedge q$（合取，"p 与 q"）和 $\neg p$（否定，"非 p"）的真值表完全相同，它们已经在 4.3 节出现过. 惟一的不同点就是用 1 和 0 分别代表着"T"和"F". 因此逻辑电路满足关于命题的定律，构成布尔代数. 正式叙述这个结论如下.

定理 15.12 逻辑电路形成一个布尔代数.

于是，用于布尔代数的所有的术语，如：补，文字，基本积，极小项，积和式，完全积和式，也可用于逻辑电路.

与-或电路

对应于布尔积和表达式的逻辑电路叫做与-或电路. 这样的电路 L 有 n 个输入：

(1) 一些输入或它们的补被送入每一个与门.

(2) 所有与门的输出被送入单个的或门.

(3) 或门的输出就是电路 L 的输出.

下面说明这种逻辑电路.

例 15.10 图 15－9 是有三个输入 A,B,C 和输出 Y 的典型的与-或电路. 不难将 Y 表达为输入 A,B,C 的布尔表达式. 首先求每个与门的输出：

(a) 第一个与门的输入是 A,B,C；因此输出为 $A\cdot B\cdot C$.

(b) 第二个与门的输入是 A,B',C；因此输出为 $A\cdot B'\cdot C$.

(c) 第三个与门的输入是 A',B；因此输出为 $A'\cdot B$.

然后所有与门输出的和就是或门的输出，也就是电路的输出 Y.

因此

$$Y=A\cdot B\cdot C+A\cdot B'\cdot C+A'\cdot B.$$

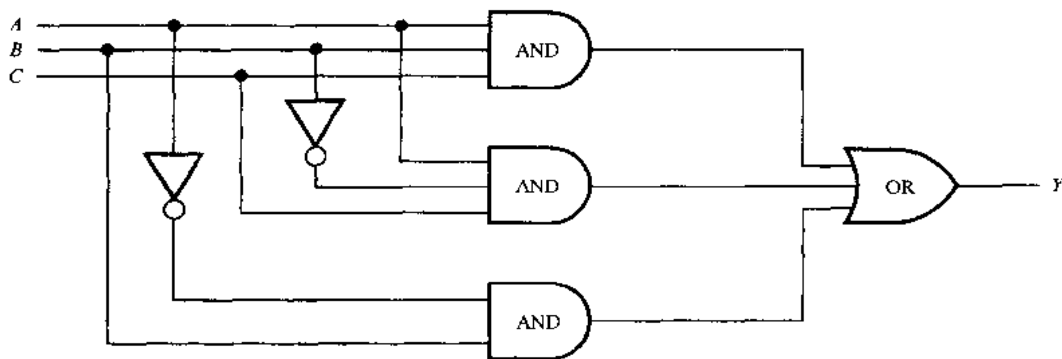


图 15－9

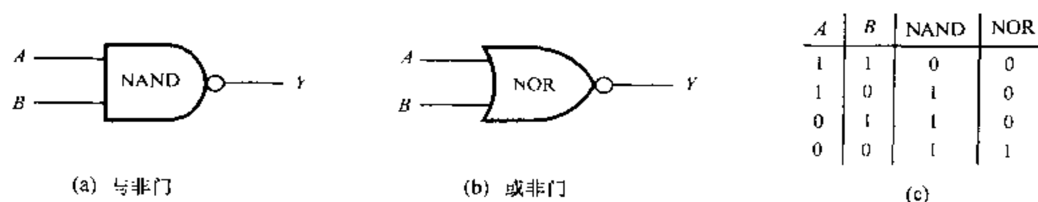
与非门和或非门

还有另外两个基本门

(a) 与非门，如图 15－10(a)所示，是一个与门后跟一个非门.

(b) 或非门，如图 15－10(b)所示，是一个或门后跟一个非门.

这些门的真值表如图 15－10(c)（两个输入 A 和 B）. 与非门和或非门实际上有两个或更多的输入，就像对应的与门和或门一样. 而且，当且仅当输入都是 1 时，与非门的输出才是 0；当且仅当输入都是 0 时，或非门的输出才是 1.



(a) 与非门 (b) 或非门

A	B	NAND	NOR
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

(c)

图 15－10

观察与门和与非门，或门和或非门之间惟一的差别是与非门和或非门都跟有一个圆圈. 有些书也在门前面使用这种小圆圈来表示补. 例如，下面的布尔表达式对应着图15－11中的逻辑电路：

(a) $Y=(A'B)'$, (b) $Y=(A'+B'+C)'$,



(a) (b)

图 15－11

15.11 真值表，布尔函数

考虑具有 $n=3$ 个输入装置 A,B,C 和输出 Y 的逻辑电路，如

$$Y=A\cdot B\cdot C+A\cdot B'\cdot C+A'\cdot B$$

把三位元集的每一个输入到 A,B,C 产生一个位元输出给 Y. 共有 $2^n=2^3=8$ 种可能按排位元输入：

$$000,001,010,011,101,110,111.$$

假定第一个位元分配给 A，第二个位元分配给 B，第三个位元分配给 C. 因此上面的输入集可重写成：

$$A=00001111, B=00110011, C=01010101.$$

我们强调这些三个 $2^n=8$－位元序列包含了输入位元的所有 8 个可能组合.

上面电路的*真值表* $T=T(L)$ 由输出序列组成，Y 对应着输入序列 A,B,C. 因此，真值表 T 可写成如下形式：

$$T(A,B,C)=Y \text{ 或 } T(L)=[A,B,C;Y].$$

如此形式的 L 的真值表本质上与 4.4 节中命题的真值表相同. 惟一的区别是这里 A,B,C 和 Y 的格式是水平书写的，而 4.4 节中是垂直书写的.

考虑一个具有 n 个输入装置的逻辑电路 L. 有许多种方法形成 n 个输入序列 $A_1,A_2,\cdots,A_n$，使得它们含有输入位元的 2^n 个不同的组合.（注意，每个序列必须含有 2^n 个位元.）下面是一个分配方案：

A₁ 分配 2^{n-1} 个位元 0，后面跟着 2^{n-1} 个位元 1.

A₂ 重复分配 2^{n-2} 个位元 0，后面跟着 2^{n-2} 个位元 1.

A₃ 重复分配 2^{n-3} 个位元 0，后面跟着 2^{n-3} 个位元 1.

等等. 以这种方法得到的序列被称为*特殊序列*. 在特殊序列中用 1 代替 0 和 0 代替 1，可得特殊序列的补.

注 假设输入是一个特殊序列，则通常对于真值表

$$T(L)=[A_1,A_2,\cdots,A_n;Y]$$

与输出 Y 不作区别.

例 15.11 (a)假设一个逻辑电路 L 有 $n=4$ 个输入装置 A,B,C,D. A,B,C,D 的 $2^n=2^4=16$－位元的特殊序列如下所示：

$$A=0000000011111111,\quad C=0011001100110011,$$
$$B=0000111100001111,\quad D=0101010101010101.$$

即

(1) A 以 8 个 0 开始后面跟着 8 个 1.(这里 $2^{n-1}=2^3=8$.)

(2) B 以 4 个 0 开始后面跟着 4 个 1,等等.(这里 $2^{n-2}=2^2=4$.)

(3) C 以 2 个 0 开始后面跟着 2 个 1,等等.(这里 $2^{n-3}=2^1=2$.)

(4) D 以 1 个 0 开始后面跟着 1 个 1,等等.(这里 $2^{n-4}=2^0=1$.)

(b) 假设一个逻辑电路 L 有 $n=3$ 个输入装置 A,B,C. A,B,C 的 $2^n=2^3=8$-位元的特殊序列和它们的补 A',B',C' 如下所示:

$$A=00001111,\quad B=00110011,\quad C=01010101,$$
$$A'=11110000,\quad B'=11001100,\quad C'=10101010.$$

下面是求逻辑电路 L 的真值表的三步算法,这里输出 Y 以输入的布尔积和式给出.

算法 15.11　输入一个布尔积和式 $Y=Y(A_1,A_2\cdots)$.

步骤 1　写出输入 $A_1,A_2\cdots$ 的特殊序列及它们的补.

步骤 2　求出现于 Y 中的每一个积.(回顾在一个位置 $x_1\cdot x_2\cdot\cdots=1$ 当且仅当在这个位置所有的 $x_1,x_2,\cdots$ 都为 1.)

步骤 3　求积的和 Y.(回顾在一个位置 $x_1+x_2+\cdots=0$ 当且仅当在这个位置所有的 $x_1,x_2,\cdots$ 都为 0.)

例 15.12　对于图 15-9 所示的逻辑电路 L,利用算法 15.11 求 L 的真值表,或等价地求布尔积和表达式

$$Y=A\cdot B\cdot C+A\cdot B'\cdot C+A'\cdot B.$$

(1) 特殊序列及其补见例 15.11(b).

(2) 积如下所示:

$$A\cdot B\cdot C=00000001,\quad A\cdot B'\cdot C=00000100,\quad A'\cdot B=00110000.$$

(3) 和 $Y=00110101$.

于是,

$$T(00001111,00110011,01010101)=00110101$$

或简单地 $T(L)=00110101$,这里我们假定输入由特殊序列组成.

布尔函数

设 E 是一个含 n 个变元 $x_1,x_2,\cdots,x_n$ 的布尔表达式.上面的讨论也可以被应用到 E 上,现在这里的特殊序列被分配到变元 $x_1,x_2,\cdots,x_n$,而不是输入装置 $A_1,A_2,\cdots,A_n$. E 的真值表 $T=T(E)$ 可如逻辑电路 L 的真值表 $T=T(L)$ 一样来定义.例如,布尔表达式

$$E=xyz+xy'z+x'y$$

和例 15.12 中的逻辑电路 L 是相类似的,产生出真值表

$$T(00001111,00110011,01010101)=00110101$$

或简单地 $T(E)=00110101$.这里我们假定输入由特殊序列组成.

注　含有 n 个变元的布尔表达式 $E=E(x_1,x_2,\cdots,x_n)$ 的真值表也可以被认为是一个从 B^n 到 B 的布尔函数.(布尔代数 B^n 和 $B=\{0,1\}$ 由例 15.1 定义.)即 B^n 中每一个元素都是 n 个位元的一个排列,而当这些排列被分配到 E 中的变元时,就能在 B 中产生出一个元素. E 的真值表 $T(E)$ 就是这个函数的一个简单图像.

例 15.13　(a) 设有含 3 个变元的布尔表达式 $E=E(x,y,z)$.八个极小项(包括 3 个变元的基

本积)如下所示：

$$xyz, xyz', xy'z, x'yz, xy'z', x'yz', x'y'z'.$$

这些极小项(对 x, y, z 用特殊序列)的真值表如下所示：

$xyz=00000001, xyz'=00000010, xy'z=00000100, x'yz=00001000,$

$xy'z'=00010000, x'yz'=00100000, x'y'z=01000000, x'y'z'=10000000.$

显然每个极小项的八个位置中只有一个值为 1.

(b) 考虑布尔表达式 $E=xyz'+x'yz+x'y'z$. 注意 E 是含有三个极小项的完全积和表达式. 因此,对 x, y, z 用特殊序列,E 的真值表 $T=T(E)$ 可以简单地从(a)中序列得到. 具体地说,E 的三个极小项中 1 所处的位置上真值表 $T(E)$ 也为 1. 因此

$$T(00001111, 00110011, 01010101)=01001010$$

或简单地 $T(E)=01001010$.

15.12 Karnaugh 图

Karnaugh 图是求至多包含 6 个变元的布尔表达式的素隐项和极小形式的一种图解法,其中关于相同变元极小项用方格来表示. 我们只讨论含两个,三个和四个变元的情况. 在 Karnaugh 图的讨论中,有时候将交替使用术语"方格"和"极小项". 我们知道极小项是一个含有所有变元的基本积而完全积和表达式则是极小项的和.

首先给出相邻积的概念. 如果 P_1 和 P_2 有相同的变元,并且它们恰好有一个文字不同,那么两个基本积 P_1 和 P_2 就称为是相邻的. 因此,在一个积中有一个变元,而在另一个积中有这个变元的补. 特别地,这样两个相邻积的和将是比原来的积少一个文字的基本积.

例 15.14 求下列相邻积 P_1 与 P_2 的和：

(a) $P_1=xyz'$ 与 $P_2=xy'z'$,

$$P_1+P_2=xyz'+xy'z'=xz'(y+y')=xz'(1)=xz'.$$

(b) $P_1=x'yzt$ 与 $P_2=x'yz't$.

$$P_1+P_2=x'yzt+x'yz't=x'yt(z+z')=x'yt(1)=x'yt.$$

(c) $P_1=x'yzt$ 和 $P_2=xyz't$.

这里 P_1 和 P_2 是不相邻的,因为它们在两个文字上不同.

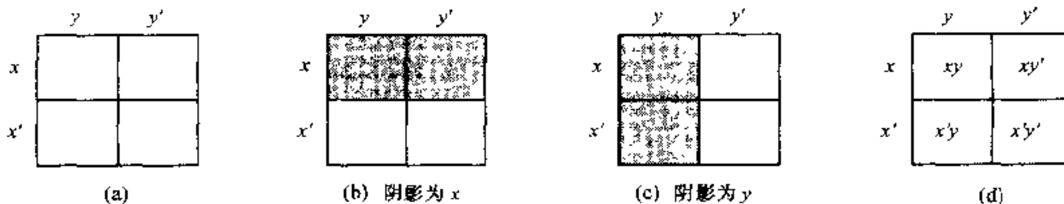
(d) $P_1=xyz'$ 和 $P_2=xyzt$.

这里 P_1 和 P_2 也是不相邻的,因为它们含有不同的变元. 这样,它们将不能以正方形的形式呈现在同一个 Karnaugh 图中.

两个变元的情形

对应于含有两个变元 x 和 y 的布尔表达式 $E=E(x,y)$ 的 Karnaugh 图,如图 15-12(a)所示. Karnaugh 图可看作是 Venn 图,这里 x 用图上半部分的点来表示,即图 15-12(b)的阴影部分. 而 y 用图左半部分的点来表示,即图 15-12(c)的阴影部分. 这样 x' 用图下半部分的点来表示,而 y' 用图右半部分的点来表示. 于是,含有两个文字的四个可能的极小项

$$xy, xy', x'y, x'y'$$



(a) (b) 阴影为 x (c) 阴影为 y (d)

图 15-12

用图中的四个方格来表示，如图 15－12(d)．正如上面定义的，两个这样的方格是相邻的，当且仅当方格在几何图形上是相邻的．(一般地认为有公共边．)

任何一个完全积和布尔表达式 $E(x,y)$ 都是极小项的和，因而可在 Karnaugh 图的适当方格处做上标记来表示．$E(x,y)$ 的素隐项将是 E 中的一对相邻方格或者是一个孤立的方格，即这个方格不和任何 $E(x,y)$ 方格相邻．$E(x,y)$ 的一个极小积和式将由盖住 $E(x,y)$ 的所有方格的极小个数的素隐项构成，下面的例子说明这一点．

例 15.15　为下面每个完全积和布尔表达式找出素隐项和一个极小积和式：

(a) $E_1=xy+xy'$；(b) $E_1=xy+x'y+x'y'$；(c) $E_1=xy+x'y'$．

这可以用下面的 Karnaugh 图来解决：

(a) 检查 xy 和 xy' 对应的方格，如图 15－13(a)所示．注意，E_1 由一个素隐项组成，即图 15－13(a)中用环标明的两个相邻方格．这对相邻方格表示变元 x，因此 x 是 E_1 的惟一的素隐项．从而，$E_1=x$ 是它的极小和．

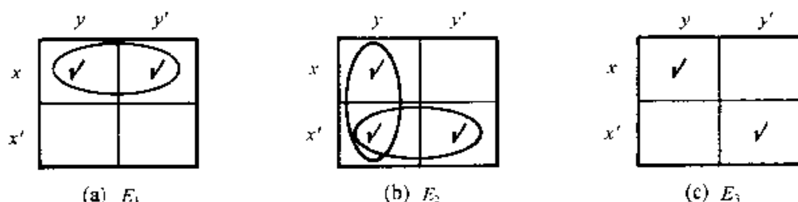


图 15－13

(b) 检查 xy，$x'y$ 和 $x'y'$ 对应的方格，如图 15－13(b)．我们注意到 E_2 包含两对相邻的方格(图中用两个环标出)，这些方格包含了 E_2 中所有的方格．垂直的一对表示 y，而水平的一对表示 x'；因此 y 和 x' 是 E_2 的两个素隐项．所以 $E_2=x'+y$ 是它的极小和．

(c) 检查 xy 和 $x'y'$ 对应的方格，如图 15－13(c)．注意到 E_3 由两个分离地表示 xy 和 $x'y'$ 的方格组成；因此，xy 和 $x'y'$ 是 E_3 的两个素隐项，并且 $E_3=xy+x'y'$ 是它的极小和．

三个变元的情形

对应着三个变元 x,y,z 的布尔表达式 $E=E(x,y,z)$ 的 Karnaugh 图，如图 15－14(a)所示．如所知，三个变元恰有 8 个极小项：

$$xyz, xyz', xy'z', xy'z, x'yz, x'yz', x'y'z', x'y'z$$

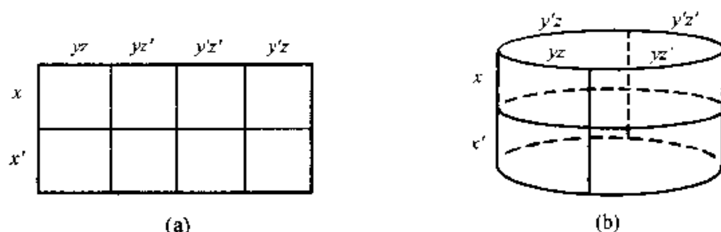


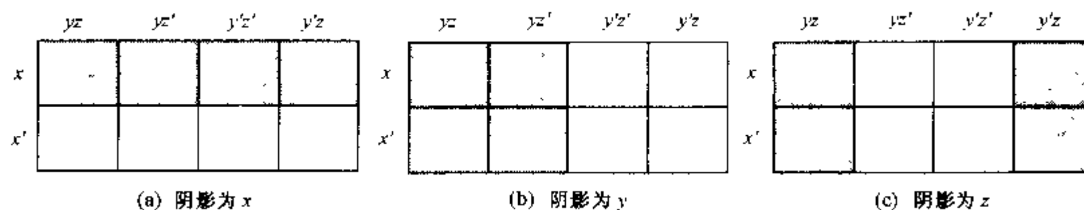
图 15－14

列出这些极小项是为了更明确地表示它们与 Karnaugh 图的对应关系．

另外，为使图 15－14(a)中的每对相邻的积按照几何方式相邻排列，我们必须让图的左边和右边变成同一条边．这等于沿着标记剪下，折叠和粘贴就可以获得一个如图 15－14(b)的圆柱．在圆柱中，相邻的积就可表示成有共用边的方格．

当把 Karnaugh 图 15－14(a)看作一个 Venn 图时，表示变元 x,y,z 的区域如图 15－15 所示．特别地，变元 x 仍由图的上半部分表示，即图 15－15(a)的阴影部分；同样变元 y 由图的左

半部分表示，如图 15-15(b)的阴影部分；新变量 z 由图的左 1/4 部分和右 1/4 部分表示，如图 15-15(c)的阴影部分. 因此，x'、y' 和 z' 分别用下半部、右半部和中间两个 1/4 部分表示.



(a) 阴影为 x　　(b) 阴影为 y　　(c) 阴影为 z

图 15-15

具有三个变元的 Karnaugh 图中的一个基本矩形，是指一个方格，两个相邻的方格或者可以组成一个 1×4 或 2×2 的矩形的 4 个方格. 这些基本矩形分别对应着 3、2 和 1 个文字的基本积. 此外，由一个基本矩形表示的基本积是由在此矩形的每个方格中都出现的文字所产生的积.

假设一个完全积和式的布尔表达式 $E=E(x,y,z)$. 用记号在 Karnaugh 图的适当的方格标记. E 的素隐项就是一个极大基本矩形. 即包含在 E 中的一个基本矩形不被 E 中任何一个其他的基本矩形所包含. E 的一个极小积和式将由 E 的一个极小覆盖构成，即极小个数的极大基本矩形一起盖住 E 的所有方格.

例 15.16　从下列完全积和布尔表达式中求素隐项和一个极小积和式：

(a) $E_1=xyz+xyz'+x'yz'+x'y'z$.

(b) $E_2=xyz+xyz'+xy'z+x'yz+x'y'z$.

(c) $E_3=xyz+xyz'+x'yz'+x'y'z'+x'y'z$.

这些可用 Karnaugh 图解答如下：

(a) 检查对应 4 个和项的方格. 如图 15-16(a)所示，观察 E_1 有 3 个素隐项(极大基本矩形)，它们已圈出；它们是 xy, yz' 和 $x'y'z$. 这三个都是覆盖 E_1 所必需的；因此 E_1 的极小和是

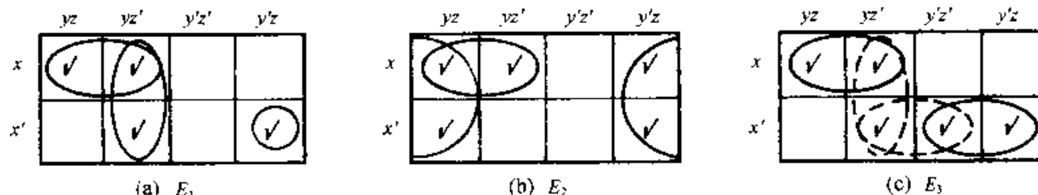
$$E_1=xy+y'z+x'y'z.$$

(b) 检查对应 5 个和项的方格，如图 15-16(b)所示，观察 E_2 有两个素隐项，它们已圈出. 一个是表示 xy 的两个相邻的方格，另一个是表示 z 的 2×2 方格. 这两个都是覆盖 E_2 所必需的；因此 E_2 的极小和是

$$E_2=xy+z.$$

(c) 检查对应 5 个和项的方格，如图 15-16(c)所示，观察 E_3 有 4 个素隐项 xy, yz', $x'z'$ 和 $x'y'$，如图中环所示. 然而 yz' 或 $x'z'$ 是 E_3 的极小覆盖所必需的，这样 E_3 有两个极小和的形式

$$E_3=xy+yz'+x'y'=xy+x'z'+x'y'.$$



(a) E_1　　(b) E_2　　(c) E_3

图 15-16

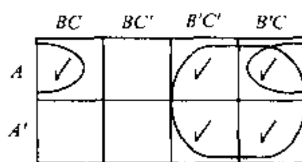
例 15.17　用下面的真值表设计一个 3-输入极小的与-或电路 L

$$T=[A,B,C;L]=[00001111,00110011,01010101;11001101].$$

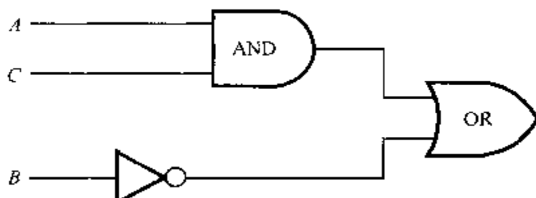
由真值表能读出 L 的完全积和式(如例 15.10)

$$L=A'B'C'+A'B'C+AB'C'+AB'C+ABC.$$

关联的 Karnaugh 图如图 15－17(a)所示. 在极小覆盖中 L 有两个素隐项 B' 和 AC. 因此 $L=B'+AC$ 是 L 的一个极小和，图 15－17(b)给出了 L 相应的极小与-或电路.



(a)



(b)

图 15－17

四个变元的情形

对应于四个变元 x,y,z,t 的布尔表达式 $E=E(x,y,z,t)$ 的 Karnaugh 图，如图15－18所示. 16 个正方形与四个变元的 16 个极小项一一对应.

$$xyzt, xyzt', xyz't', xyz't, \cdots, x'yz't$$

可由方格的行列标号表示. 观察上面和左边的标记使得相邻的积正好有一个字不同. 于是又必须把左边和右边看作同一条边(如处理三个变元的情形)，而此时还必须把上边和底边看作同一边.

在一个具有四个变元的 Karnaugh 图中，一个基本矩形就是一个方格，两个相邻的方格，四个方格组成的 1×4 或 2×2 矩形，或 8 个方格组成的一个 2×4 矩形. 这些矩形分别与有着 4,3,2 和 1 个文字的基本积相对应. 再一次极大基本矩形就是素隐项. 布尔表达式 $E(x,y,z,t)$ 的极小化技巧和前面相同.

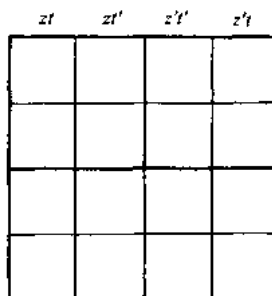
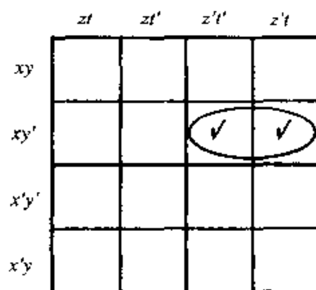
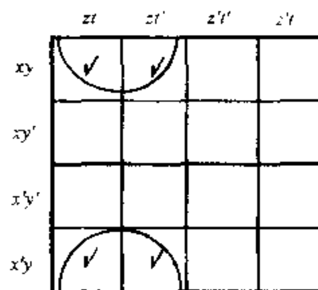


图 15－18

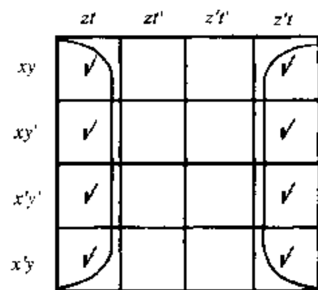
例 15.18　在 Karnaugh 图 15－19 中找出由基本矩形所示的基本积 P.



(a)



(b)



(c)

图 15－19

对于每一种情况，求得出现在基本矩形中所有方格中的文字；P 是由这些文字产生的积.

(a) x, y' 和 z' 出现在两个方格中，因此 $P=xy'z'$.

(b) 仅有 y 和 z 出现在所有的四个方格中，因此 $P=yz$.

(c) 仅有 t 出现在所有的八个方格中，因此 $P=t$.

例 15.19　用 Karnaugh 图求 E 的极小积和式

$$E=xy'+xyz+x'y'z'+x'yzt'.$$

检查表示每个基本积的所有方格，即标出表示 xy' 的四个方格，表示 xyz 的两个方格，表示 $x'y'z'$ 的两个方格和表示 $x'yzt'$ 的一个方格，如图 15－20 所示. 图的一个极小覆盖由做了标记的三个极大基本矩形构成. 那个 2×2 方格表示基本积 xz 和 $y'z'$，另外两

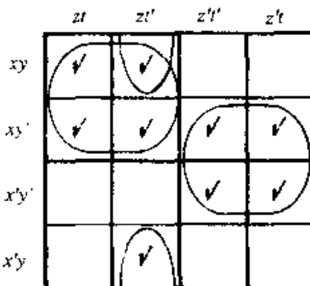


图 15－20

个相邻的方格(上部和底部)表示 yzt'. 因此,

$$E=xz+y'z'+yzt'$$

是 E 的一个极小和.

问题与解答

布尔代数

15.1 写出每个布尔等式的对偶式:

(a) $(a*1)*(0+a')=0$; (b) $a+a'b=a+b$.

解 ☞ (a) 要得到对偶式,把+和*交换,把0和1交换,得到

$$(a+0)+(1*a')=1.$$

(b) 首先用*号写等式得 $a+(a'*b)=a+b$,这样对偶式是 $a*(a'+b)=a*b$,也可写成

$$a(a'+b)=ab.$$

15.2 回顾(第十四章),m 的因数集 $\mathbf{D}_m$ 是一个有界分配格,具有 $a+b=a\vee b=\mathrm{lcm}(a,b)$ 和 $a*b=a\wedge b=\gcd(a,b)$. (a) 如果 m 是无平方因子数,即 m 是不同素数的积,证明 $\mathbf{D}_m$ 是一个布尔代数. (b)求 $\mathbf{D}_m$ 的原子.

证 ☞ (a) 只要证明 $\mathbf{D}_m$ 是有补格. 设 $x\in\mathbf{D}_m$ 和 $x'=m/x$. 既然 m 是不同素数的积,x 和 x' 有不同的素数因子. 因此 $x*x'=\gcd(x,x')=1$ 和 $x+x'=\mathrm{lcm}(x,x')=m$. 回顾1是 $\mathbf{D}_m$ 的0元素(即下界)和 m 是 $\mathbf{D}_m$ 的单位元素(即上界). 这样 x' 是 x 的一个补,所以 $\mathbf{D}_m$ 是一个布尔代数.

(b) $\mathbf{D}_m$ 的原子是 m 的素数因子.

15.3 考虑布尔代数 $\mathbf{D}_{210}$.

(a) 列出它的元素并画出 Hasse 图.

(b) 求原子集合 A.

(c) 求两个具有8个元素的子代数.

(d) $X=\{1,2,6,210\}$ 是 $\mathbf{D}_{210}$ 的一个子格吗? 一个子代数吗?

(e) $Y=\{1,2,3,6\}$ 是 $\mathbf{D}_{210}$ 的一个子格吗? 一个子代数吗?

解 ☞ (a) 210的因数是1,2,3,5,6,7,10,14,15,21,30,35,42,70,105和210. $\mathbf{D}_{210}$ 的 Hasse 图如图15-21所示.

(b) $A=\{2,3,5,7\}$ 是210的素因数的集合.

(c) $B=\{1,2,3,35,6,70,105,210\}$ 和 $C=\{1,5,6,7,30,35,42,210\}$ 是 $\mathbf{D}_{210}$ 的子代数.

(d) X 是一个子格,因为它是线性排序的. 然而 X 不是子代数,因为35是 $\mathbf{D}_{210}$ 中2的补,但是35不属于 X.(事实上,没有一个具有两个或两个以上元素的布尔代数是线性排序的.)

(e) Y 是 $\mathbf{D}_{210}$ 的一个子格,因为它关于+与*封闭. 然而,Y 不是 $\mathbf{D}_{210}$ 的一个子代数,因为它对 $\mathbf{D}_{210}$ 中的补不封闭. 例如,$35=2'$ 不属于 Y.(注意 Y 本身是一个布尔代数,事实上 $Y=\mathbf{D}_6$.)

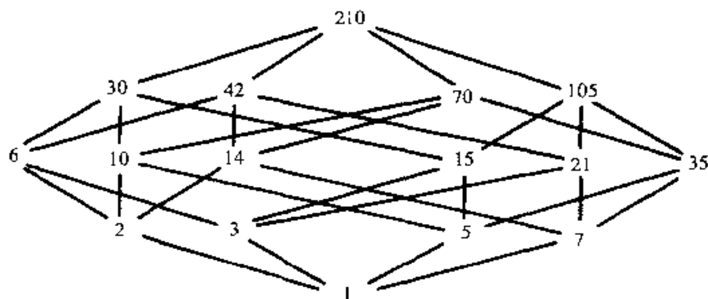


图15-21

15.4 求 $\mathbf{D}_{210}$ 中子代数的个数.

解 ☞ $\mathbf{D}_{210}$ 中的一个子代数必须包含2个、4个、8个或16个元素.

(i) 只可能有一个两元素子代数，包含上界 210 和下界 1，即$\{1,210\}$.

(ii) 因为 $\mathbf{D}_{210}$ 包含 16 个元素，故惟一的具有 16 个元素的子代数即为 $\mathbf{D}_{210}$ 本身.

(iii) 任何一个含 4 个元素的子代数都具有$\{1,x,x',210\}$的形式，即包含着上界和下界，而且还有一个非上、下界元素和它的补. $\mathbf{D}_{210}$ 中有 14 个非上、下界元素，所以有 $14/2=7$ 对$\{x,x'\}$. 这样 $\mathbf{D}_{210}$ 就有 7 个含 4 个元素的子代数.

(iv) 任一个 8 元素的子代数 S 本身都将含 3 个原子 s_1,s_2,s_3. 可选 s_1,s_2 为 $\mathbf{D}_{210}$ 的 4 个原子中的两个，然后 s_3 必为另外两个原子的积. 例如，可设 $s_1=2,s_2=3,s_3=5\cdot 7=35$(由上述子代数 B 决定). 或者设 $s_1=5,s_2=7,s_3=2\cdot 3=6$(由决定上述子代数 C). 这里有 $\binom{4}{2}=6$ 种方式从 $\mathbf{D}_{210}$ 中的四个原子中选择 s_1 和 s_2. 于是 $\mathbf{D}_{210}$ 有 6 个 8 元素子代数.

综上所述，$\mathbf{D}_{210}$ 有 $1+1+7+6=15$ 个子代数.

15.5　证明定理 15.2：设 a,b,c 为布尔代数 B 中的任意元素.

(i) 幂等律：

(5a) $a+a=a$；(5b) $a*a=a$.

(ii) 有界律：

(6a) $a+1=1$；(6b) $a*0=0$.

(iii) 吸收律：

(7a) $a+(a*b)=a$；(7b) $a*(a+b)=a$.

(iv) 结合律：

(8a) $(a+b)+c=a+(b+c)$；(8b) $(a*b)*c=a*(b*c)$.

证 ☞　(5b) $a=a*1=a*(a+a')=(a*a)+(a*a')=(a*a)+0=a*a$.

(5a) 由 (5b) 和对偶性得.

(6b) $a*0=(a*0)+0=(a*0)+(a*a')=a*(0+a')=a*(a'+0)=a*a'=0$.

(6a) 由(6b)和对偶性得.

(7b) $a*(a+b)=(a+0)*(a+b)=a+(0*b)=a+(b*0)=a+0=a$.

(7a) 由(7b)和对偶性得.

(8b) 设 $L=(a*b)*c$ 和 $R=a*(b*c)$. 我们来证 $L=R$. 先证 $a+L=a+R$. 最后一步运用吸收律

$$a+L=a+((a*b)*c)=(a+(a*b))*(a+c)=a*(a+c)=a.$$

同样，在最后一步也运用吸收律

$$a+R=a+(a*(b*c))=(a+a)*(a+(b*c))=a*(a+(b*c))=a.$$

因此，$a+L=a+R$. 下面我们指出 $a'+L=a'+R$.

$$\begin{aligned}a'+L&=a'+((a*b)*c)=(a'+(a*b))*(a'+c)\\&=((a'+a)*(a'+b))*(a'+c)=(1*(a'+b))*(a'+c)\\&=(a'+b)*(a'+c)=a'+(b*c).\end{aligned}$$

同样，

$$\begin{aligned}a'+R&=a'+(a*(b*c))=(a'+a)*(a'+(b*c))\\&=1*(a'+(b*c))=a'+(b*c).\end{aligned}$$

于是，可得 $a'+L=a'+R$. 所以

$$\begin{aligned}L&=0+L=(a*a')+L=(a+L)*(a'+L)=(a+R)*(a'+R)\\&=(a*a')+R=0+R=R.\end{aligned}$$

(8a)由(8b)和对偶性得.

15.6　证明定理 15.3：设 a 为布尔代数 B 中的任一元素.

(i)（补的惟一性）如果 $a+x=1$ 且 $a*x=0$，那么 $x=a'$.

(ii)（对合律）$(a')'=a$.

(iii) (9a) $0'=1$，(9b) $1'=0$.

证 ☞　(i) 我们有

$$a'=a'+0=a'+(a*x)=(a'+a)*(a'+x)$$

$$=1*(a'+x)=a'+x,$$

且

$$x=x+0=x+(a*a')=(x+a)*(x+a')$$
$$=1*(x+a')=x+a'.$$

因此，

$$x=x+a'=a'+x=a'.$$

(ii) 根据补的定义，$a+a'=1$ 且 $a*a'=0$. 根据交换律，$a'+a=1$ 且 $a'*a=0$. 根据补的惟一性，a 是 a' 的补，即 $a=(a')'$.

(iii) 根据有界律(6a)，$0+1=1$，同理(3b)，$0*1=0$. 根据补的惟一性，1 是 0 的补，即 $1=0'$ 根据对偶性，$0=1'$.

15.7 证明定理 15.4 (DeMorgan 律) (10a) $(a+b)'=a'*b'$；(10b) $(a*b)'=a'+b'$.

证 ☞ (10a) 我们要证明 $(a+b)+(a'*b')=1$ 和 $(a+b)*(a'*b')=0$；然后根据补的惟一性，有 $a'*b'=(a+b')$. 我们有：

$$(a+b)+(a'*b')=b+a+(a'*b')=b+(a+a')*(a+b')$$
$$=b+1*(a+b')=b+a+b'$$
$$=b+b'+a=1+a=1.$$

也有

$$(a+b)*(a'*b')=((a+b)*a')*b'$$
$$=((a*a')+(b*a'))*b'=(0+(b*a'))*b'$$
$$=(b*a')*b'=(b*b')*a'=0*a'=0.$$

因此

$$a'*b'=(a+b)'.$$

(10b) 对偶原理(定理 15.1).

15.8 证明定理 15.5：下面式子在布尔代数中等价：
(1) $a+b=b$，(2) $a*b=a$，(3) $a'+b=1$，(4) $a*b'=0$.

证 ☞ 根据定理 14.4，(1)和(2)等价. 现在证明(1)和(3)等价. 假设(1)成立，那么

$$a'+b=a'+(a+b)=(a'+a)+b=1+b=1.$$

现假设(3)成立，那么

$$a+b=1*(a+b)=(a'+b)*(a+b)=(a'*a)+b=0+b=b.$$

因此(1)和(3)等价.

下面证明(3)和(4)等价. 假设(3)成立，根据 DeMorgan 律和对合律，

$$0=1'=(a'+b)'=a''*b'=a*b'.$$

反过来，如果(4)成立，那么

$$1=0'=(a*b')'=a'+b''=a'+b.$$

因此(3)和(4)等价. 所以，4 个式子均等价.

15.9 证明定理 15.6：映射 $f:B\to P(A)$ 是一个同构映射，其中 B 是布尔代数，$P(A)$ 是原子集 A 的幂集. 且

$$f(x)=\{a_1,a_2,\cdots,a_n\}.$$

这里 $x=a_1+\cdots+a_n$ 是 a 作为原子和的惟一表达.

证 ☞ 回忆第十四章有，如果 $a_1,a_2,\cdots,a_n$ 是原子，那么 $a_i^2=a_i(i=1,2,\cdots,n)$；但是对于 $a_i\neq a_j$，$a_ia_j=0$. 假设 x,y 属于 B，并且假设

$$x=a_1+\cdots+a_r+b_1+\cdots+b_s,$$
$$y=b_1+\cdots+b_s+c_1+\cdots+c_t.$$

这里

$$A=\{a_1,\cdots,a_r,b_1,\cdots b_s,c_1,\cdots,c_t,d_1,\cdots,d_k\}$$

是 B 中原子的集合，则

$$x+y=a_1+\cdots+a_r+b_1+\cdots+b_s+c_1+\cdots+c_t,$$
$$xy=b_1+\cdots+b_s.$$

因此

$$f(x+y)=\{a_1,\cdots,a_r,b_1,\cdots,b_s,c_1,\cdots,c_t\}$$
$$=\{a_1,\cdots,a_r,b_1,\cdots,b_s\}\cup\{b_1,\cdots,b_s,c_1,\cdots,c_t\}$$
$$=f(x)\cup f(y).$$
$$f(xy)=\{b_1,\cdots,b_s\}$$
$$=\{a_1,\cdots,a_r,b_1,\cdots,b_s\}\cap\{b_1,\cdots,b_s,c_1,\cdots,c_t\}$$
$$=f(x)\cap f(y).$$

令：

$$y=c_1+\cdots+c_t+d_1+\cdots+d_k,$$

那么　$x+y=1$ 且 $xy=0.$

因此，$y=x'$

故

$$f(x')=\{c_1,\cdots,c_t,d_1,\cdots,d_k\}=\{a_1,\cdots,a_r,b_1,\cdots,b_s\}^c=(f(x))^c$$

因为表示是惟一的，f 为一对一和映上的映射，所以 f 是布尔代数的同构映射.

布尔表达式

15.10　化简下列布尔积为 0 或基本积：

(a) $xyx'z$；(b) $xyzy$；(c) $xyz'yx$；(d) $xyz'yx'z'$.

解　利用交换律 $x*y=y*x$，补律 $x*x'=0$ 和幂律 $x*x=x$：

(a) $xyx'z=xx'yz=0yz=0.$

(b) $xyzy=xyyz=xyz.$

(c) $xyz'yx=xxyyz'=xyz'.$

(d) $xyz'yx'z'=xx'yyz'z'=0yz'=0.$

15.11　把下列布尔表达式 $E(x,y,z)$ 表示为积和式，并且用它的完全积和式表示.

(a) $E=x(xy'+x'y+y'z)$；(b) $E=z(x'+y)+y'$.

解　首先用算法 15.8A 来表示 E 的积和式，然后用算法 15.8B 来表示 E 的完全积和式.

(a) 首先，我们有 $E=xxy'+xx'y+xy'z=xy'+xy'z$. 然后

$$E=xy'(z+z')+xy'z=xy'z+xy'z'+xy'z=xy'z+xy'z'.$$

(b) 首先，我们有 $E=z(x'+y)+y'=x'z+yz+y'$. 然后

$$E=x'z+yz+y'=x'z(y+y')+yz(x+x')+y'(x+x')(z+z')$$
$$=x'yz+x'y'z+xyz+x'yz+xy'z+xy'z'+x'y'z+x'y'z$$
$$=xyz+xy'z+xy'z'+x'yz+x'y'z+x'y'z'.$$

15.12　将 $E(x,y,z)=(x'+y)'+x'y$ 表示成完全积和式.

解　我们有 $E=(x'+y)'+x'y=xy'+x'y$，如果 E 是 x 和 y 的布尔表达式，那么 E 已经是完全积和式. 然而，E 是 x,y,z 三种变元的布尔表达式. 因此

$$E=xy'+x'y=xy'(z+z')+x'y(z+z')=xy'z+xy'z'+x'yz+x'yz'$$

是 E 的完全积和式.

15.13　把下列布尔表达式 $E(x,y,z)$ 表示为积和式，然后表示为完全积和式

(a) $E=y(x+yz)'$；(b) $E=x(xy+y'+x'y)$.

解　(a) $E=y(x'(yz)')=yx'(y'+z')=yx'y'+x'yz'=x'yz'$ 且已为完全积和式.

(b) 首先，$E=xxy+xy'+xx'y=xy+xy'$，然后，

$$E=xy(z+z')+xy'(z+z')=xyz+xyz'+xy'z+xy'z'.$$

15.14　把下列集合表达式 $E(A,B,C)$ 改写为交的并：

(a) $E=(A\cup B)^c\cap(C^c\cup B)$；(b) $E=(B\cap C)^c\cap(A^c\cap C)^c$.

解　利用布尔符号，$'$ 表示补，$+$ 表示并，$*$ 表示交，然后把 E 表示成积和式（交集的并）

(a) $E=(A+B)'(C'+B)=A'B'(C'+B)=A'B'C'+A'B'B=A'B'C'$ 或 $E=A^c\cap B^c\cap C^c$；

(b) $E=(BC)'(A'+C)'=(B'+C')(AC')=AB'C'+AC'$ 或 $E=(A\cap B^c\cap C^c)\cup(A\cap C^c)$.

15.15 设 $E=xy'+xyz'+x'yz'$. 证明：

(a) $xz'+E=E$；(b) $x+E\neq E$；(c) $z'+E\neq E$.

证 ☞ 因为完全积和式是惟一的，$A+E=E$，其中 $A\neq 0$，当且仅当 A 的完全积和式的加项在 E 的完全积和式的加项中．因此，首先求 E 的完全积和式

$$E=xy'(z+z')+xyz'+x'yz'=xy'z+xy'z'+xyz'+x'yz'.$$

(a) 表示 xz' 的完全积和式

$$xz'=xz'(y+y')=xyz'+xy'z'.$$

因为 xz' 的加项在 E 的加项中，所以有 $xz'+E=E$.

(b) 表示 x 的完全积和式

$$x=x(y+y')(z+z')=xyz+xyz'+xy'z+xy'z'.$$

x 的加项 xyz 不是 E 的加项，因此 $x+E\neq E$.

(c) 表示 z' 的完全积和式

$$z'=z'(x+x')(y+y')=xyz'+xy'z'+x'yz'+x'y'z'.$$

z' 的加项 $x'y'z'$ 不是 E 的加项，因此 $z'+E\neq E$.

极小布尔表达式，素隐项

15.16 对于任何布尔积和表达式 E，设 E_L 表示 E 中文字的数目，E_S 表示 E 中被加项的数目．求下列各式的 E_L 与 E_S：

(a) $E=xy'z+x'z'+yz'+x$；　　(b) $E=x'y'z+xyz+y+yz'+x'z$；

(c) $E=xyt'+x'y'zt+xz't$；　　(d) $E=(xy'+z)'+xy'$.

解 ☞ 只需把每个式中加项的文字数相加且数出加项的数目：

(a) $E_L=3+2+2+1=8$，$E_S=4$.

(b) $E_L=3+3+1+2+2=11$，$E_S=5$.

(c) $E_L=3+4+3=10$，$E_S=3$.

(d) 因为 E 不是积和式，E_L 和 E_S 无定义.

15.17 已知 E 和 F 是等价的布尔积和式，定义：

(a) E 比 F 简单；(b) E 是极小的.

解 ☞ (a) E 比 F 简单，如果 $E_L<F_L$ 且 $E_S\leqslant F_S$ 或 $E_L\leqslant F_L$ 且 $E_S<F_S$.

(b) E 是极小的，如果没有与 E 等价的且比 E 简单的积和式.

15.18 求基本积 P_1 和 P_2 的共识 Q：

(a) $P_1=xy'z'$，$P_2=xyt$；　　(b) $P_1=xyz't$，$P_2=xzt$；

(c) $P_1=xy'z'$，$P_2=x'y'zt$；　　(d) $P_1=xyz'$，$P_2=xz't$.

解 ☞ 当存在惟一变元 x_k，它的补出现在 P_1 或 P_2 中，而它的非补出现在另一个中，那么 P_1 和 P_2 的共识 Q 存在，而且 Q 是 P_1 和 P_2 在 x_k 和 x_k' 被删之后的文字的积(无重复).

(a) 删除 y' 和 y，再把 P_1 和 P_2 相乘(无重复)，得 $Q=xz't$.

(b) 删除 z' 和 z，得 $Q=xyt$.

(c) 因为 x 和 z 中每一个在一式中为补，在另一式中为非补，所以它们没有共识.

(d) 因为没有一个变元以补形式出现在一式，以非补形式出现在另一式，所以它们没有共识.

15.19 证明引理 15.10：假设 Q 是 P_1 和 P_2 的共识，则 $P_1+P_2+Q=P_1+P_2$.

证 ☞ 因为文字可交换，不失一般性，假设

$$P_1=a_1a_2\cdots a_rt,\ P_2=b_1b_2\cdots b_st',\ Q=a_1a_2\cdots a_rb_1b_2\cdots b_s.$$

则 $Q=Q(t+t')=Qt+Qt'$. 因为 Qt 包含 P_1，$P_1+Qt=P_1$，而且 Qt' 包含 P_2，$P_2+Qt'=P_2$，所以

$$P_1+P_2+Q=P_1+P_2+Qt+Qt'=(P_1+Qt)+(P_2+Qt')=P_1+P_2.$$

15.20 设 $E=xy'+xyz'+x'yz'$. 求：(a) E 的素隐项；(b) E 的极小和.

解 ☞ (a) 运用算法 15.9A(共识方法)如下

$E=xy'+xyz'+x'yz'+xz'$　（xy'和xyz'的共识）
$=xy'+x'yz'+xz'$　（xyz'包含xz'）
$=xy'+x'yz'+xz'+yz'$　（$x'yz'$和xz'的共识）
$=xy'+xz'+yz'.$　（$x'yz'$包含yz'）

共识方法不能再用.因此xy',xz'和yz'为E的素隐项.

(b) 运用算法15.9B.把E的每个素隐项写成完全积和式

$$xy'=xy'(z+z')=xy'z+xy'z',$$
$$xz'=xz'(y+y')=xyz'+xy'z',$$
$$yz'=yz'(x+x')=xyz'+x'yz'.$$

仅xz'的被加项xyz'和$xy'z'$出现在其他被加项中,所以xz'可以作为多余而删除.因此$E=xy'+yz'$为E的极小和.

15.21 设$E=xy+y't+x'yz'+xy'zt'$.求(a)E的素隐项;(b)E的极小和.

解☞ (a) 运用算法15.9A(共识方法)如下

$E=xy+y't+x'yz'+xy'zt'+xzt'$　（xy和$xy'zt'$的共识）
$=xy+y't+x'yz'+xzt'$　（$xy'zt'$包含xzt'）
$=xy+y't+x'yz'+xzt'+yz'$　（xy和$x'yz'$的共识）
$=xy+y't+xzt'+yz'$　（$x'yz'$包含yz'）
$=xy+y't+xzt'+yz'+xt$　（xy和$y't$的共识）
$=xy+y't+xzt'+yz'+xt+xz$　（xzt'和xz的共识）
$=xy+y't+yz'+xt+xz$　（xzt'包含xt）
$=xy+y't+yz'+xt+xz+z'.$　（$y't$和yz'的共识）

共识方法不能再用,因此E的素隐项为xy,$y't$,yz'.xt,xz和$z't$.

(b) 运用算法15.9B.即写出每一个素隐项的完全积和式,然后消去多余的素隐项.最后结果

$$E=y't+xz+yz'$$

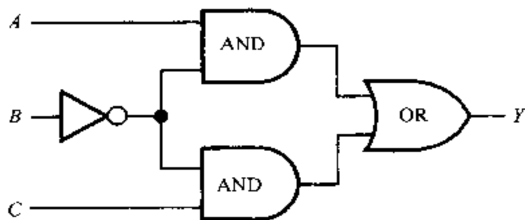
是E的极小和.

逻辑门

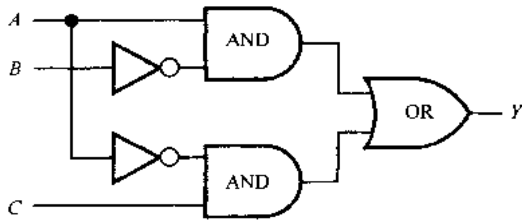
15.22 将下列逻辑电路的输出Y表示成输入A,B,C的布尔表达式:(a)图15-22(a);(b)图15-22(b).

解☞ (a) 第一个与门的输入是A和B',第二个与门的输入是B'和C.因此$Y=AB'+B'C$.

(b) 第一个与门的输入是A和B',第二个与门的输入是A'和C.因此$Y=AB'+A'C$.



(a)



(b)

图15-22

15.23 将图15-23所示的逻辑电路的输出Y表示成输入A,B,C的布尔表达式.

解☞ 第一个与门的输出是$A'BC$,第二个与门的输出是$AB'C'$,最后一个与门的输出是AB'.因此,

$$Y=A'BC+AB'C'+AB'.$$

15.24 将下列逻辑电路的输出Y表示成输入A,B,C的布尔表达式:(a)图15-24(a);(b)图15-24(b).

解☞ (a) 与门的输出是BC,所以或非门的输入是A和BC.因此或非门的输出是$(A+BC)'$.所

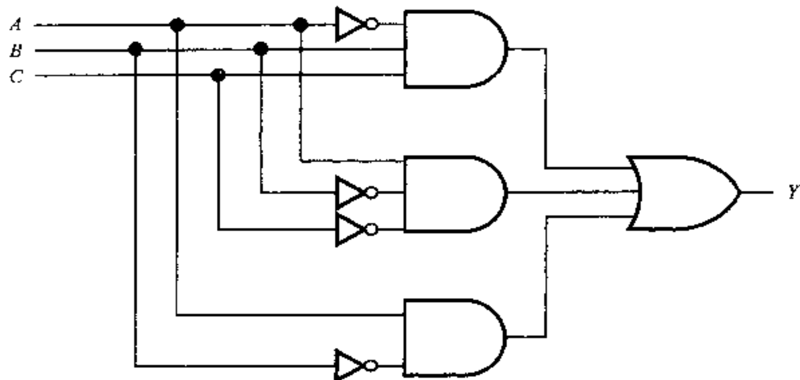


图 15 - 23

以或门的输入是$(A+BC)'$和 B. 因此 $Y=(A+BC)'+B$.

(b) 与非门的输出是$(A'B)'$，或非门的输出是$(A+C)'$，因此 $Y=(A'B)'+(A+C)'$.

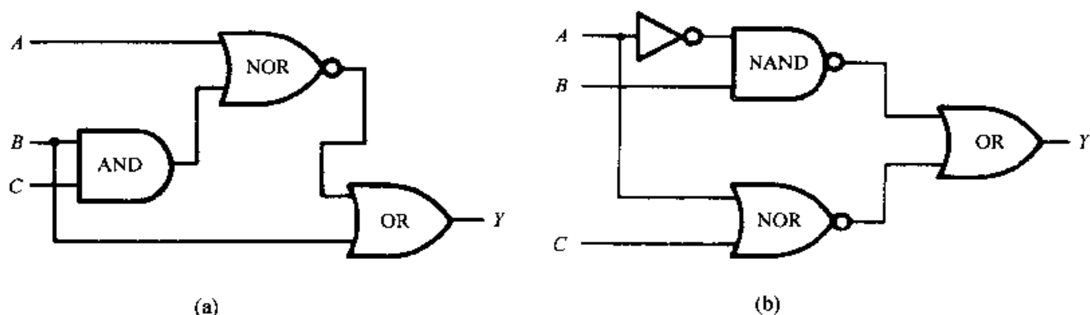


图 15 - 24

15.25 将图 15 - 25 所示逻辑电路的输出 Y 表示成输入 A 和 B 的布尔表达式.

解 这里电路中的小圈表示补. 所以左边三个门的输出分别是 AB'，$(A+B)'$，$(A'B)'$. 因此：

$$Y=AB'+(A+B)'+(A'B)'.$$

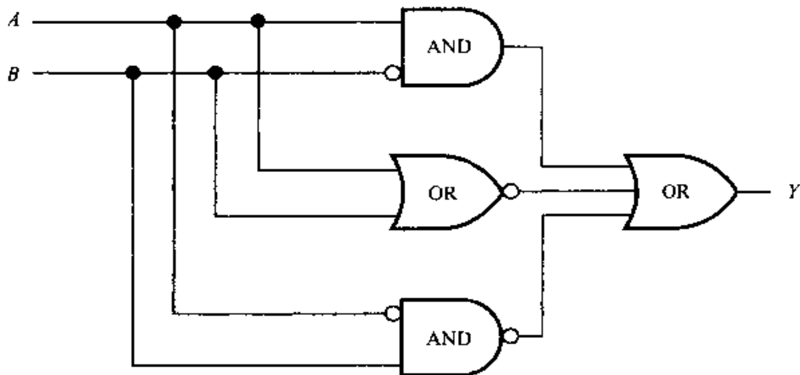


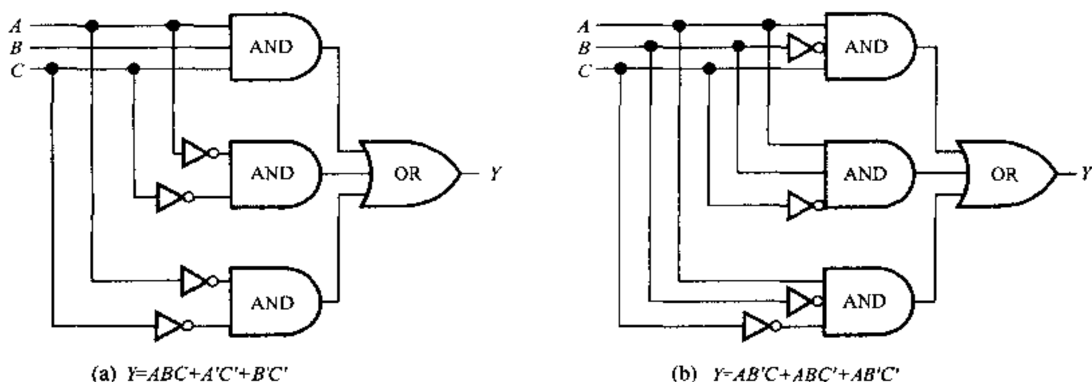
图 15 - 25

15.26 画出逻辑电路 L，L 的输入是 A，B，C，输出为 Y，且 Y 相应的布尔表达式分别是
(a) $Y=ABC+A'C'+B'C'$；(b) $Y=AB'C+ABC'+AB'C'$.

解 上述式子均为积和式. 所以 L 是一个与-或电路，且一个积对应一个与门，一个和对应一个或门. 所求电路如图 15 - 26(a)，15 - 26(b)所示.

真值表

15.27 求输入是 A，B，C 的与门(或等价地写成 $Y=ABC$)的输出序列 Y. 其中：
(a) $A=111001$，$B=100101$，$C=110011$.



(a) $Y=ABC+A'C'+B'C'$　　(b) $Y=AB'C+ABC'+AB'C'$

图 15 - 26

(b) $A=11111100, B=10101010, C=00111100$.

(c) $A=00111111, B=11111100, C=11000011$.

解 当且仅当输入序列各位都是 1 时，与门的输出是 $Y=1$. 因此：

(a) 三个序列都只有第一位和最后一位是 1，故 $Y=100001$.

(b) 三个序列都只有第三位和第五位(从左向右数)是 1，故 $Y=00101000$.

(c) 三个序列各位都不是 1，故 $Y=00000000$.

15.28 求输入是 A,B,C 的或门(或等价地写成 $Y=A+B+C$)的输出序列 Y. 其中

(a) $A=100001, B=100100, C=110000$.

(b) $A=11000000, B=10101010, C=00000011$.

(c) $A=00111111, B=11111100, C=11000011$.

解 当且仅当输入序列各位都是 0 时，或门的输出是 $Y=0$. 因此

(a) 三个序列都只有第三位和第五位是 0，故 $Y=110101$.

(b) 三个序列都只有第四位和第六位(从左向右数)是 0. 故 $Y=11101011$.

(c) 三个序列各位都不是 0. 故 $Y=11111111$.

15.29 求输入是 A 的非门(或等价地写成 $Y=A'$)的输出序列 Y. 其中

(a) $A=00111111$, (b) $A=11111100$, (c) $A=11000011$.

解 非门将 0 变为 1，将 1 变为 0，因此

(a) $A'=11000000$, (b) $A'=00000011$, (c) $A'=00111100$.

15.30 考虑一个逻辑电路 L，L 有 $n=5$ 个输入：A,B,C,D,E. 或者等价地说，即考虑一个布尔表达式 E，E 有 5 个变元 x_1,x_2,x_3,x_4,x_5.

(a) 求变元(输入)的特殊序列.

(b) 可以有多少种方法来给 $n=5$ 个变元分配位元(0 或 1)?

(c) 特殊序列的主要性质是什么?

解 (a) 所有序列的长都是 $2^n=2^5=32$. 它们由交替的 0 块和 1 块组成，其中块的长度分别为 $x_1:2^{n-1}=2^4=16, x_2:2^{n-2}=2^3=8, \cdots, x_5:2^{n-5}=2^0=1$. 因此

$$x_1=00000000000000001111111111111111,$$
$$x_2=00000000111111110000000011111111,$$
$$x_3=00001111000011110000111100001111,$$
$$x_4=00110011001100110011001100110011,$$
$$x_5=01010101010101010101010101010101.$$

(b) 给一个变元分配位元有两种方法(0 或 1)，所以给 $n=5$ 个变元分配位元有 $2^n=2^5=32$ 种方法.

(c) 特殊序列的 32 个位置给 5 个变元以 32 种可能的位元组合方式.

15.31 求布尔表达式 $E=E(x,y,z)$ 的真值表 $T=T(E)$. 其中(a) $E=xz+x'y$; (b) $E=$

$xy'z+xy+z'$.

解 ☞　变元 x,y,z 及其补的特殊序列如下

$$x=00001111, y=00110011, z=01010101,$$
$$x'=11110000, y'=11001100, z'=10101010.$$

(a) 这里 $xz=00000101$, $x'y=00110000$. 从而 $E=xz+x'y=00110101$. 因此

$$T(00001111, 00110011, 01010101)=00110101.$$

或当我们设定输入由特殊序列组成时，可简单地写成 $T(E)=00110101$.

(b) 这里 $xy'z=00000100$, $xy=00000011$, $z'=01010101$. 从而 $E=xy'z+xy+z'=01010111$. 因此

$$T(00001111, 00110011, 01010101)=01010111.$$

15.32　求布尔表达式 $E=E(x,y,z)$ 的真值表 $T=T(E)$. 其中(a) $E=xyz'+x'yz$, (b) $E=xyz+xy'z+x'y'z$.

解 ☞　这里 E 是极小项的和的完全积和式. 例 15.13 给出了极小项的真值表(用特殊序列). 每个极小项的真值表包含一个 1；因此 E 的真值表与 E 的极小项在相同的位置上出现 1.

(a) $T(E)=00001010$, (b) $T(E)=01000101$.

15.33　求布尔表达式 $E=E(x,y,z)=(x'y)'yz'+x'(yz+z')$ 的真值表 $T=T(E)$.

解 ☞　首先将 E 表示成积和式

$$E=(x+y')yz'+x'yz+x'z'=xyz'+y'yz'+x'yz+x'z'$$
$$=xyz'+x'yz+x'z'.$$

再将 E 表示成完全积和式

$$E=xyz'+x'yz+x'z'(y+y')$$
$$=xyz'+x'yz+x'yz'+x'y'z'.$$

如同问题 15.32，利用例 15.13 中出现的极小项的真值表可得 $T(E)=10101010$.

15.34　求下列真值表相应的布尔表达式

(a) $T(E)=01001001$, (b) $T(E)=00010001$.

解 ☞　$T(E)$ 中的每个 1 对应着极小项的相同位上的 1(利用例 15.13 极小项的真值表). 例如，第二位的 1 对应着 $x'y'z$ 的真值表的第二位的 1. 从而 E 是这些极小项的和. 因此.

(a) $E=x'y'z+x'yz+xyz'$, (b) $E=xy'z'+xyz$.

(我们仍然设定输入由特殊序列组成.)

Karnaugh 图

15.35　求图 15－27 中 Karnaugh 图的每个基本矩形所表示的基本积.

解 ☞　只要找到那些出现在基本矩形的所有方格里的文字，那么 P 就是这些文字的积.

(a) x' 和 z' 都出现在两个方格中，所以 $P=x'z'$.

(b) x 和 z 都出现在两个方格中，所以 $P=xz$.

(c) 只有 z 出现在所有四个方格中，所以 $P=z$.

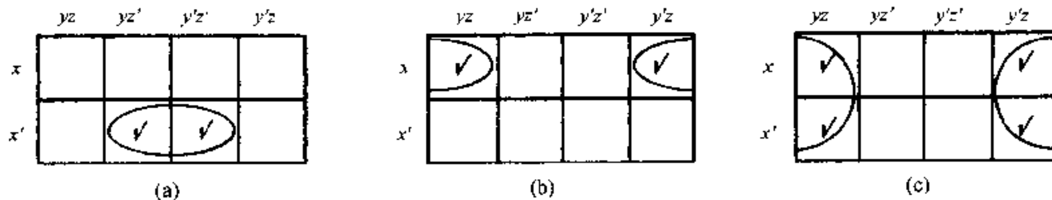


图 15－27

15.36　设 R 是变元 x,y,z,t 的 Karnaugh 图中的一个基本矩形. 用 R 中方格的数目叙述对应于 R 的基本积 P 的文字的数目.

解 ☞　R 有 8,4,2 或 1 个方格，相应地，P 有 1,2,3 或 4 个文字.

15.37　求图 15－28 中 Karnaugh 图的每个基本矩形所表示的基本积 P.

解 ☞　只要找到那些出现在基本矩形所有方格里的文字，那么 P 就是这些文字的积.（问题 15.36 指出了 P 中这些文字的数目.）

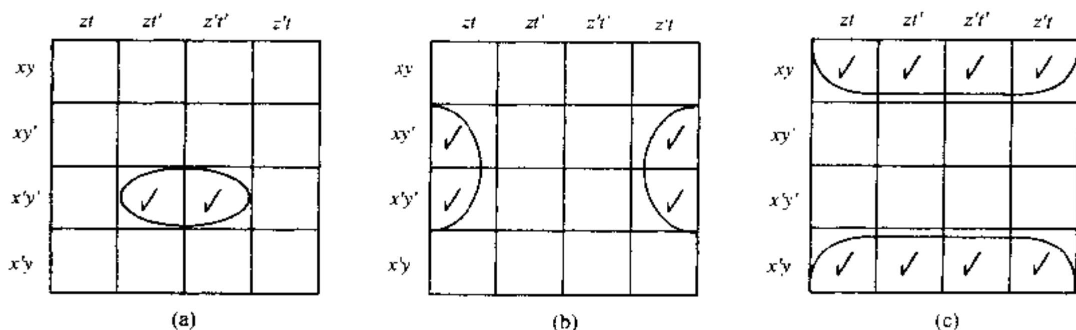


图 15－28

(a) R 中有 2 个方格，从而 P 中有 3 个文字. 具体地说，x'、y'、t' 都在每个方格中出现，所以 $P=x'y't'$.

(b) R 中有 4 个方格，从而 P 中有 2 个文字. 具体地说，只有 y' 和 t 在全部四个方格中出现，所以 $P=y't$.

(c) R 中有 8 个方格，从而 P 中只有 1 个文字. 具体地说，只有 y 在全部八个方格中出现，所以 $P=y$.

15.38　设 E 是图 15－29 所示 Karnaugh 图给出的布尔表达式

(a) 把 E 写成完全积和式，(b) 求 E 的极小式.

解 ☞　(a) 列出七个基本积，得

$$E=xyz't'+xyz't+xy'zt+xy'zt'+x'y'zt-x'y'zt'+x'yz't'.$$

(b) 图中 2×2 极大基本矩形表示 $y'z$，因为只有 y' 和 z 出现在所有四个方格中. 而一对水平相邻的方格表示 xyz'，覆盖顶边和底边的相邻方格表示 $yz't'$. 因为所有这 3 个矩形对于极小覆盖都是必需的，所以

$$E=y'z+xyz'+yz't'$$

是 E 的极小和.

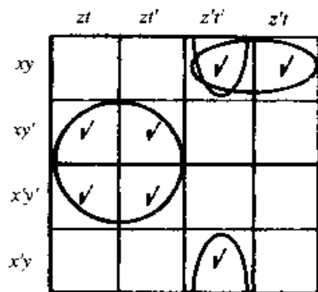
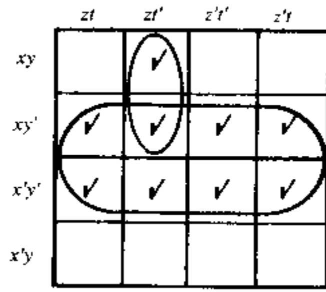
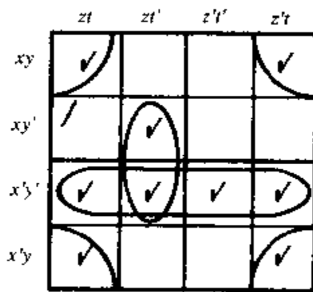


图 15－29



(a) E_1



(b) E_2

图 15－30

15.39　在图 15－30 所示 Karnaugh 图中，考虑以变元 x,y,z,t 表示的布尔表达式 E_1 和 E_2. 求(a) E_1 的极小和，(b) E_2 的极小和.

解 ☞　(a) 在图中标出的 2×4 极大基本矩形中，只有 y' 出现在全部八个方格中，且其中一对带标记的相邻方格表示 xzt'. 因为两个矩形对于极小覆盖都是必需的，所以

$$E_1=y'+xzt'$$

是 E_1 的极小和.

(b) 四个角上的方格形成了一个 2×2 的极大基本矩形，表示 yt，因为只有 y 和 t 出现在所有四个方格中. 另有 4×1 极大基本矩形表示 $x'y'$，而两个相邻的方格代表 $y'zt'$. 因为这三个矩形对于极小

覆盖都是必需的，所以

$$E_2 = yt + x'y' + y'zt'$$

是 E_2 的极小和.

15.40 在图 15－31 所示 Karnaugh 图中，考虑变元 x,y,z,t 的布尔表达式 E_1, E_2，求(a) E_1 的极小和，(b) E_2 的极小和.

解 (a) 这里有五个素隐项，由四个环和一个虚线圈标记. 然而虚线圈是多余的，四个环却是必需的. 因此，这四个环给出了 E_1 的极小和，即

$$E = xzt' + xy'z' + x'y'z + x'z't'.$$

(b) 这里有五个素隐项，由五个环标记，其中有两个是虚线环. 要覆盖方格 $x'y'z't'$ 只须这两个虚线环中的一个. 因此 E_2 有两个极小和，如下

$$E_2 = x'y + yt + xy't' + y'z't' = x'y + yt + xy't' + x'z't'.$$

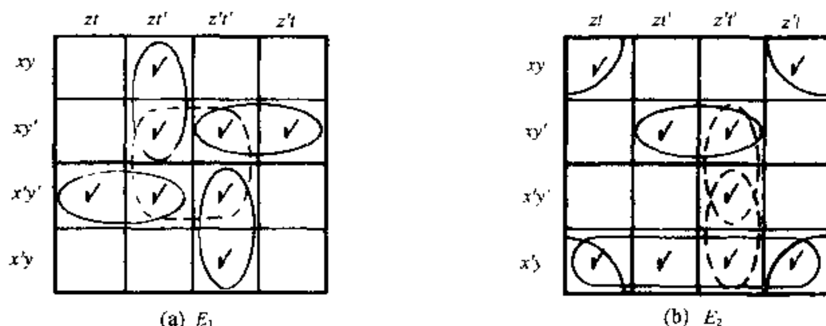


图 15－31

15.41 用 Karnaugh 图求下列各式的极小和：

(a) $E_1 = x'yz + x'yz't + y'zt' + xyzt' + xy'z't'$.

(b) $E_2 = y't' + y'z't + x'y'zt + yzt'$.

解 (a) 标出对应 $x'yz$ 和 $y'zt'$ 的两个方格，再标出对应于 $x'yz't$、$xyzt'$ 和 $xy'z't'$ 的方格. 这样可作出如图 15－32(a)所示的 Karnaugh 图. 一个极小覆盖由 3 个标记环组成. 因此 E_1 的极小和如下

$$E_1 = zt' + xy't' + x'yt.$$

(b) 标出对应 zt' 的 4 个方格、对应 $y'z't$ 和 yzt' 的两个方格以及对应 $x'y'zt$ 的方格. 这就给出了如图 15－32(b)所示的 Karnaugh 图. 一个极小覆盖由 3 个标记的极大基本矩形组成. 所以 E_2 的极小和如下

$$E_2 = zt' + xy't' + x'yt.$$

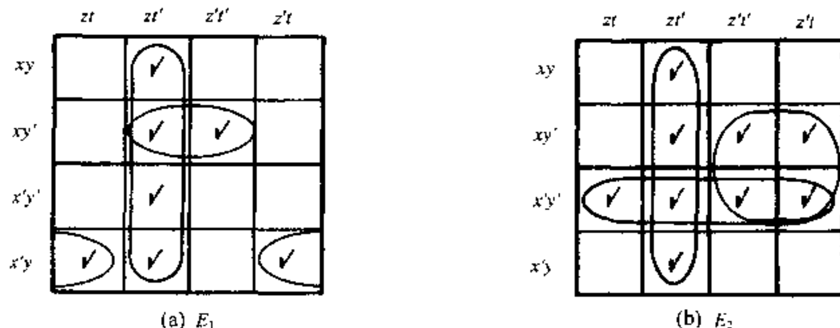


图 15－32

15.42 用下列真值表求布尔表达式 E 的一个极小积和式：

(a) $T(00001111, 00110011, 01010101) = 10100110$,

(b) $T(00001111, 00110011, 01010101) = 00101111$.

解 (a) 由给定真值表 T(和例 15.13 中用变元 x,y,z 表示的极小项的真值表)可得 E 的完全

积和式

$$E=x'y'z'+x'yz'+xy'z+xyz'.$$

它的 Karnaugh 图如图 15 - 33(a)所示. 这里有三个素隐项，由三个环标记，形成了 E 的极小覆盖，因此 E 的极小式为

$$E=yz'+x'z'+xy'z$$

(b) 由给定真值表可得 E 的完全积和式

$$E=x'yz'+x'yz+xy'z+xyz'+xyz.$$

它的 Karnaugh 图如图 15 - 33(b)所示. 这里有两个素隐项，由两个环标记，形成了 E 的极小覆盖，因此 E 的极小式为

$$E=xz+y.$$

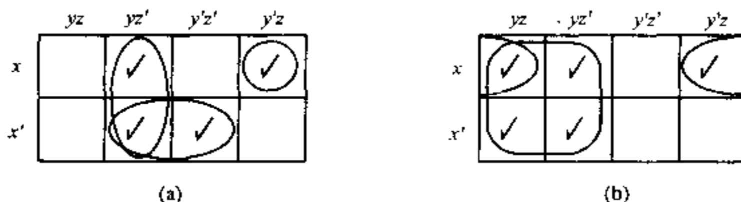


图 15 - 33

补　充　题

布尔代数

15.43 写出布尔表达式的对偶式.

(a) $a(a'+b)=ab$.

(b) $(a+1)(a+0)=a$.

(c) $(a+b)(b+c)=ac+b$.

15.44 考虑 m 因数的格 $\mathbf{D}_m(m>1)$.

(a) 证明 $\mathbf{D}_m$ 是一个布尔代数，当且仅当 m 是没有平方因子的数，即：当 m 是不同的素数之积.

(b) 若 $\mathbf{D}_m$ 是一布尔代数，证明它的原子是 m 的不同的素因数.

15.45 考虑下面的格：(a) $\mathbf{D}_{20}$，(b) $\mathbf{D}_{55}$，(c) $\mathbf{D}_{99}$，(d) $\mathbf{D}_{130}$. 哪些是布尔代数，它们的原子是什么？

15.46 考虑布尔代数 $\mathbf{D}_{110}$，(a) 列出它的元素并画出它的 Hasse 图. (b) 求其所有子代数. (c) 求四元子格的数目. (d) 求 $\mathbf{D}_{110}$ 的原子集合 A. (e) 按定理 15.6 中定义，给出同构映射 $f:\mathbf{D}_{110}\to P(A)$.

15.47 设 B 是一布尔代数. 证明：

(a) 对于 B 中任一 x，$0\leqslant x\leqslant 1$.

(b) $a<b$，当且仅当 $b'<a'$.

15.48 布尔代数中的一个元素 x 被称为极大项，如果单位元是它惟一的后继元. 求图 15 - 21 中布尔代数 $\mathbf{D}_{210}$ 的极大项.

15.49 设 B 是一布尔代数. (a) 证明 B 中原子的补元是极大项. (b) 证明 B 中的元素 x 能惟一地表示为极大项的积.

15.50 设 B 是一个 16 元素布尔代数，S 是 B 的一个 8 元素子代数，证明 S 中有两个原子一定是 B 的原子.

15.51 设 $B=(B,+,*,',0,1)$是一布尔代数. 用

$$x\Delta y=(x*y')+(x'*y)$$

来定义 B 的 Δ 运算(称作对称差).

证明：$R=(B,\Delta,*)$是一个交换布尔环(见 12.6 节问题 12.77).

15.52 设 $R=(R,\oplus,\cdot)$是带有单位元 $1\neq 0$ 的布尔环，定义：

$$x'=1\oplus x,\ x+y=x\oplus y\oplus x\cdot y,\ x*y=x\cdot y.$$

证明：$B=(R,+,*,',0,1)$是一布尔代数.

布尔表达式，素隐项

15.53 化简下面的布尔积为 0 或一个基本积：

(a) $xy'zxy'$.　(b) $xyz'sy'ts$.　(c) $xy'xz'ty'$,　(d) $xyz'ty't$.

15.54 将布尔表达式 $E(x,y,z)$ 表示为积和式，再表示成完全积和式：

(a) $E=x(xy'+x'y+y'z)$,　(b) $E=(x+y'z)(y+z')$,

(c) $E=(x'+y)'+y'z$.

15.55 将布尔表达式 $E(x,y,z)$ 表示为积和式，再表示成完全积和式：

(a) $E=(x'y)'(x'+xyz')$,　(b) $E=(x+y)'(xy')'$,

(c) $E=y(x+yz)'$.

15.56 求基本积 P_1 和 P_2 的共识 Q.

(a) $P_1=xy'z, P_2=xyt$.　(b) $P_1=xyz't', P_2=xzt'$.

(c) $P_1=xy'zt$, $P_2=xyz'$.　(d) $P_1=xy't$, $P_2=xzt$.

15.57 对任意布尔积和式 E，设 E_L 表示 E 中文字的数目（重复计算），E_S 表示 E 中加项的个数. 求 E_L、E_S：

(a) $E=xyz't+x'yt+xy'zt$,　(b) $E=xyzt+xt'+x'y't+yt$.

15.58 运用共识方法（算法 15.9A），求布尔表达式的素隐项.

(a) $E_1=xy'z'+x'y+x'y'z'+x'yz$.

(b) $E_2=xy'+x'z't+xyzt'+x'y'zt'$.

(c) $E_3=xyzt+xyz't'+xz't'+x'y'z'+x'yz't$.

15.59 求问题 15.58 中布尔表达式的极小积和式.

逻辑门，真值表

15.60 对下面的逻辑电路，用以输入 A,B,C 作为变元的布尔表达式来表示输出 Y.

(a) 图 15－34(a),　(b) 图 15－34(b).

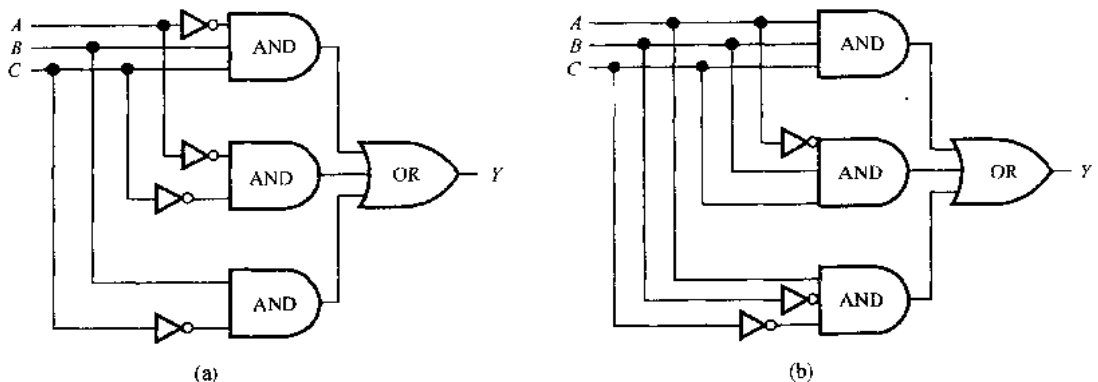


图 15－34

15.61 对下面的逻辑电路，用以输入 A,B,C 作为变元的布尔表达式表示输出 Y.

(a) 图 15－35(a),　(b) 图 15－35(b).

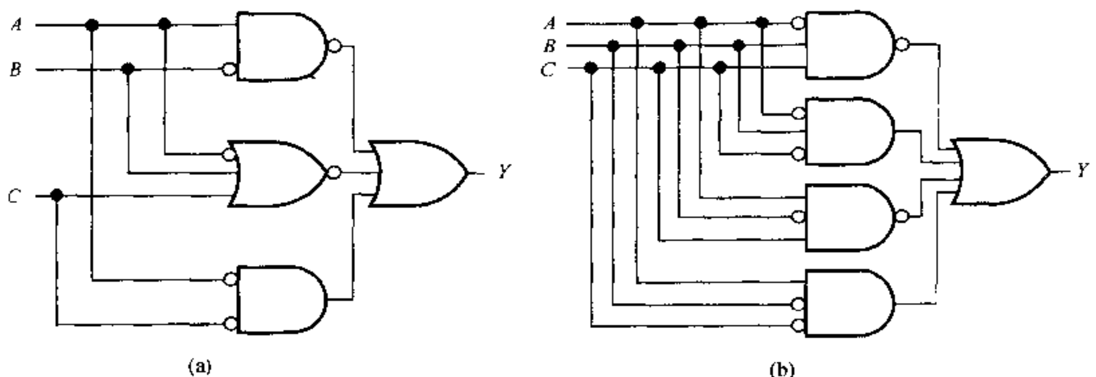


图 15－35

15.62 画出对应于下面布尔表达式的逻辑电路 L，L 的输入为 A,B,C，输出为 Y.

(a) $Y=AB'C+AC'+B'C$.　(b) $Y=A'BC+A'BC'+ABC'$.

15.63　对于输入 A,B,C 的与门(等价于 $Y=ABC$),求输出序列 Y:

(a) $A=110001$; $B=101101$; $C=110011$.

(b) $A=01111100$; $B=10111010$; $C=00111100$.

(c) $A=00111110$; $B=01111100$; $C=11110011$.

15.64　对于输入 A,B,C 的或门(等价于 $Y=A+B+C$),求输出序列 Y.

(a) $A=100011$; $B=100101$; $C=1000001$.

(b) $A=10000001$; $B=00100100$; $C=00000011$.

(c) $A=00111100$; $B=11110000$; $C=10000001$.

15.65　对于输入 A 的非门(等价于 $Y=A'$),求输出序列:

(a) $A=11100111$;　　(b) $A=10001000$;　　(c) $A=11111000$.

15.66　考虑有 6 个输入 A,B,C,D,E,F 的逻辑电路 L,或等价地,考虑有 6 个变元 x_1,x_2,x_3,x_4,x_5,x_6 的布尔表达式 E.

(a) 有多少种方法将位元(0 或 1)分配给 6 个变元?

(b) 求变元(输入)前三个特殊序列.

15.67　求布尔表达式 $E=E(x,y,z)$ 的真值表 $T=T(E)$.

(a) $E=xy+x'z$,　　(b) $E=xyz'+y+xy'$.

15.68　求布尔表达式 $E=E(x,y,z)$ 的真值表 $T=T(E)$.

(a) $E=x'yz'+x'y'z$,　　(b) $E=xyz'+xy'z'+x'y'z'$.

15.69　求对应于真值表的布尔表达式 $E=E(x,y,z)$.

(a) $T(E)=10001010$,　(b) $T(E)=00010001$,　(c) $T(E)=00110000$.

15.70　求图 15-36 所示 Karnaugh 图给出的布尔表达式的所有可能的极小和.

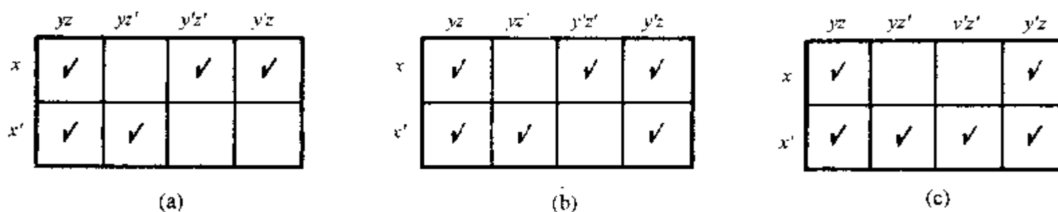


图 15-36

15.71　求图 15-37 所示 Karnaugh 图给出的布尔表达式的所有可能的极小和.

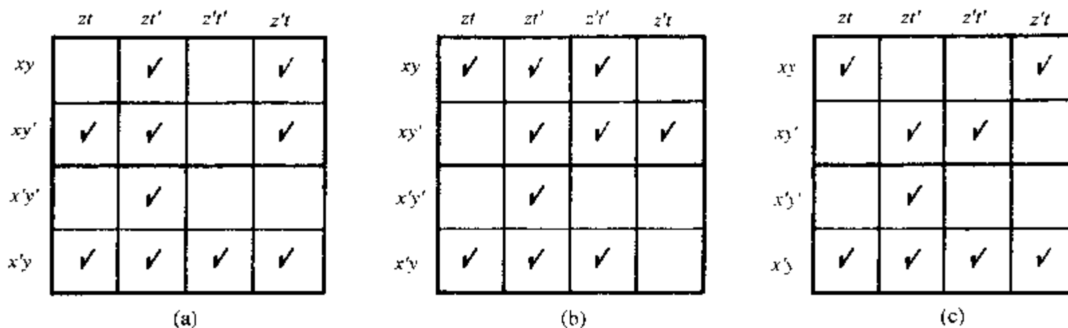


图 15-37

15.72　利用 Karnaugh 图求布尔表达式的极小和:

(a) $E=xy+x'y+x'y'$;　　(b) $E=x+x'yz+xy'z'$.

15.73　求布尔表达式的极小和:

(a) $E=y'z+y'z't'+z't$;　　(b) $E=y'zt+xzt'+xy'z'$.

15.74　用 Karnaugh 图重新设计图 15-38 所示逻辑电路 L,使之成为极小的与-或电路.

15.75　假设三个开关与大厅里同一个灯相连,在任何时候,一个开关"向上"用 1 表示,"向下"用 0 表示. 任何一个开关变化将改变 1 的个数的奇偶性. 当 1 的个数为奇数时,表示灯亮,当 1 的个数为偶数时,灯不亮.

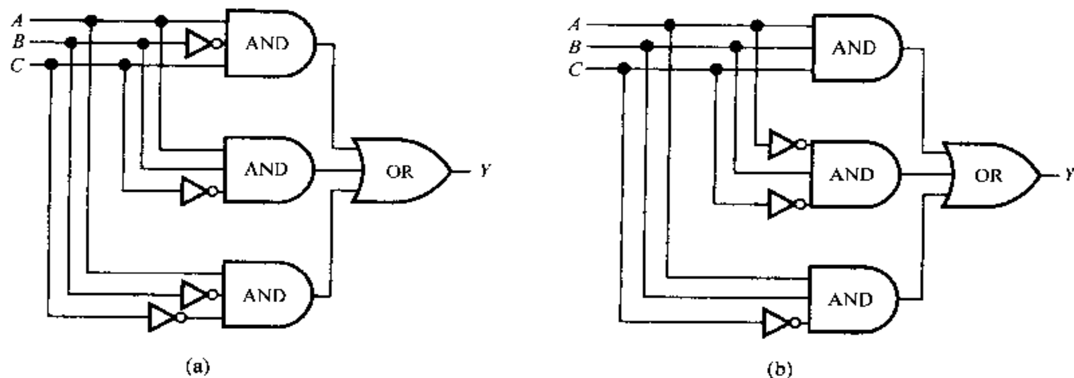


图 15－38

(a) 证明：下面的真值表满足这些条件

$$T(A,B,C)=T(00001111,00110011,01010101)=01101001.$$

(b) 用上面的真值表设计一个极小的与-或逻辑电路 L.

补充题答案

15.43　(a) $a+a'b=a+b$.

(b) $a\cdot 0+a\cdot 1=a$.

(c) $ab+bc=(a+c)b$.

15.45　(b) $\mathbf{D}_{55}$；原子 5 和 11.　(d) $\mathbf{D}_{130}$；原子 2、5 和 13.

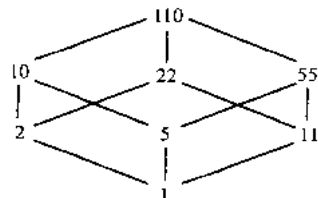
15.46　(a) 有 8 个元素：1,2,5,10,11,22,55,110. 见图 15－39(a).

(b) 有 5 个子代数：{1,110}，{1,2,55,110}，{1,5,22,110}，{1,10,11,110}，$\mathbf{D}_{110}$.

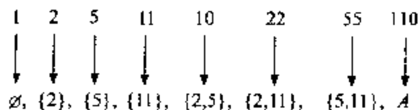
(c) 有 15 个子格，它们包含上面三个子代数.

(d) $A=\{2,5,11\}$.

(e) 见图 15－39(b).



(a) $\mathbf{D}_{110}$



(b) $f:\mathbf{D}_{110}\longrightarrow P(A)$

图 15－39

15.48　极大项：30,42,70,105.

15.49　(b) 提示：用对偶性.

15.53　(a) $xy'z$；　(b)0；　(c) $xy'z't$；　(d)0.

15.54　(a) $E=xy'+xy'z=xy'z'+xy'z$.

(b) $E=xy+xz'=xyz+xyz'+xy'z'$.

(c) $E=xy'+y'z=xy'z+xy'z'+x'y'z$.

15.55　(a) $E=xyz'+x'y'=xyz'+x'y'z+x'y'z'$.

(b) $E=x'y'=x'y'z+x'y'z'$.

(c) $E=x'yz'$.

15.56　(a) $Q=xzt$；　(b) $Q=xyt'$；　(c) 不存在；　(d)不存在.

15.57　(a) $E_L=11, E_S=3$；(b) $E_L=11, E_S=4$.

15.58　(a) $x'y, x'z', y'z'$.

(b) $xy', xzt', y'zt', x'z't, y'z't$.

(c) $xyzt, xz't', y'z't', x'y'z', x'z't$.

15.59 (a) $E=x'y+x'z'$.

(b) $E=xy'+xzt'+x'z't+y'z't$.

(c) $E=xyzt+xz't'+x'y'z'+x'z't$.

15.60 (a) $Y=A'BC+A'C'+BC'$; (b) $Y=A+B+C+A'BC+AB'C'$.

15.61 (a) $Y=(AB')'+(A'+B+C)'+AC$.

(b) $Y=(A'BC)'+A'BC'+(AB'C)'+AB'C'$.

15.62 见图 15－40.

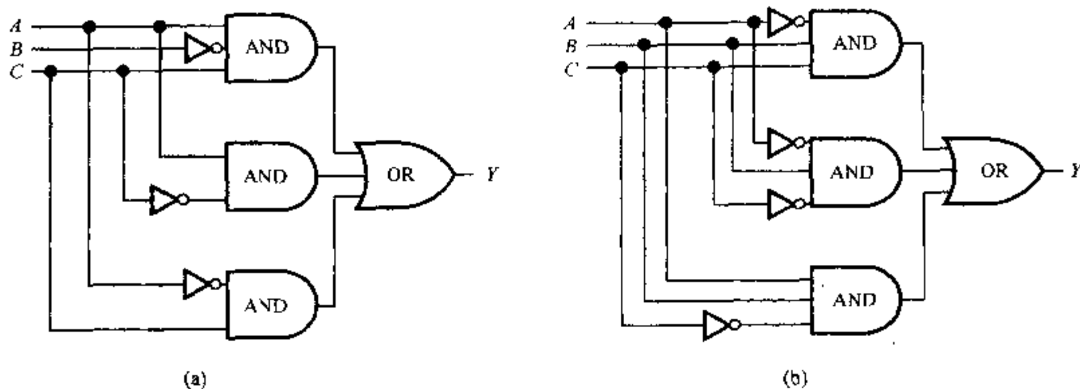


图 15－40

15.63 (a) $Y=100001$; (b) $Y=00111000$; (c) $Y=00110000$.

15.64 (a) $Y=100111$; (b) $Y=10100111$; (c) $Y=11111101$.

15.65 (a) $A'=00011000$; (b) $A'=01110111$; (c) $A'=00000111$.

15.66 (a) $2^n=2^6=64$

(b) $x_1=000\cdots00111\cdots11$ (32 个 0)(32 个 1),

$x_2=(00000000000000001111111111111111)^2$,

$x_3=(0000000011111111)^4$.

15.67 (a) $T(E)=01010011$; (b) $T(E)=00111111$.

15.68 (a) $T(E)=01000000$; (b) $T(E)=10001010$.

15.69 对例 15.13 的极小项用真值表.

(a) $E=x'y'z'+xyz'+xyz'$.

(b) $E=xy'z'+xyz$.

(c) $E=x'yz'+xy'z'$.

15.70 (a) $E=xy'+x'y+yz=xy'+x'y+xz'$.

(b) $E=xy'+x'y+z$.

(c) $E=x'+z$.

15.71 (a) $E=x'y+zt'+xz't+xy'z=x'y+zt'+xz't+xy't$.

(b) $E=yz+yt'+zt'+xy'z'$.

(c) $E=x'y+yt+xy't'+x'zt=x'y+yt+xy't'+y'zt$.

15.72 (a) $E=x'+y$; (b) $E=xz'+yz$.

15.73 (a) $E=y'+z't$; (b) $E=xy'+zt'+y'zt$.

15.74 (a) 见图 15－41.

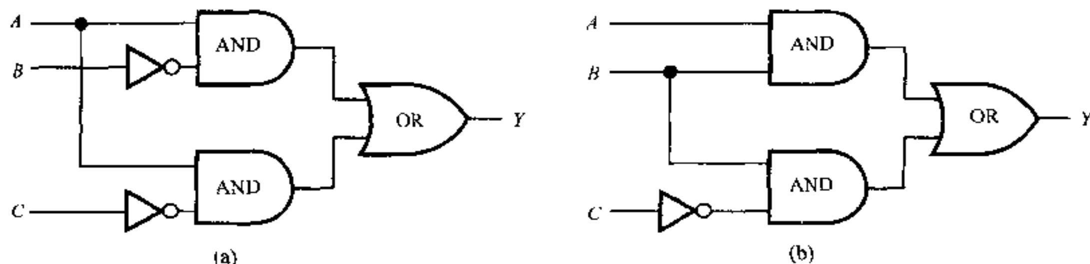


图 15－41

15.75 (b) 见图 15－42.

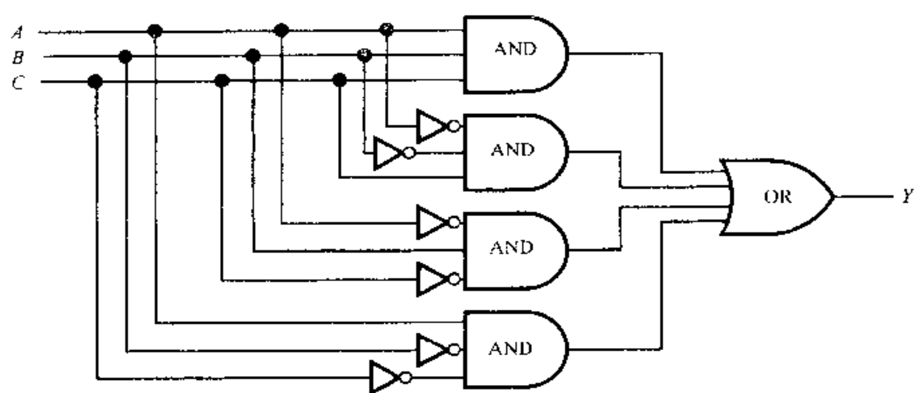


图 15－42